



STATE OF MICHIGAN PROCUREMENT
 Department Technology, Management and Budget
 Central Procurement Services
 320 S Walnut Street Lansing, MI 48933
 P.O. Box 30026, Lansing, MI 48909

CONTRACT CHANGE NOTICE

Change Notice Number **3**
 to
 Contract Number **MA230000001430**

CONTRACTOR	JEM TECH GROUP
	23537 Lakepointe Drive
	Clinton Twp MI 48036
	Jami Moore
	586-783-3400
	j.moore@jemtechgroup.com
	CV0032887

STATE	Program Manager	Eric Haas	DTMB
		(517) 449-5858	
		HaasE@michigan.gov	
	Contract Administrator	Lauren Stempek	DTMB
		(517) 243-4008	
		StempekL@Michigan.gov	

CONTRACT SUMMARY

Hardware and software for the Enterprise Operations Center-Data Center for Visitor Management, Asset Control and Physical Audit, Rack Locking, and Environmental Monitoring.

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
September 1, 2023	August 31, 2028	5 - 1 Year	December 31, 2028

PAYMENT TERMS	DELIVERY TIMEFRAME
n/a	n/a

ALTERNATE PAYMENT OPTIONS	EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (PRC) <input type="checkbox"/> Other	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS
n/a

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>	0 Years	
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$3,566,463.70	\$0.00	\$3,566,463.70		

DESCRIPTION

Please note the Program Manager or Contract Administrator may have changed, and are reflected on this Change Notice.

Effective 3/12/2026, The State is required to comply with the Americans with Disabilities Act of 1990 (ADA) and has adopted standards and procedures regarding accessibility requirements for websites, applications, content, and electronic documents. Due to a change in the law, the State is required to comply with specific accessibility standards for websites, applications, content and documents.

Starting 4/24/2026, throughout the Term, all websites, applications, software, content, and electronic documents, including but not limited to mobile applications, text, images, sounds, videos, controls, animations, links, and documents (including files in the following formats: PDF, word processing, presentation, and spreadsheet), created must comply with WCAG 2.1 Level AA.

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Central Procurement Services approval.



STATE OF MICHIGAN ENTERPRISE PROCUREMENT

Department of Technology, Management, and Budget
320 S. Walnut Street 2nd Floor Lansing, MI 48933
P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number 2
to
Contract Number MA230000001430

CONTRACTOR	JEM TECH GROUP
	23537 Lakepointe Drive
	Clinton Twp MI 48036
	Jami Moore
	586-783-3400
	j.moore@jemtechgroup.com
	CV0032887

STATE	Program Manager	Jennifer Poirier	DTMB
		517-242-2417	
		PoirierJ@Michigan.gov	
	Contract Administrator	Lauren Stempek	DTMB
(517) 243-4008			
stempekL@Michigan.gov			

CONTRACT SUMMARY

Hardware and software for the Enterprise Operations Center-Data Center for Visitor Management, Asset Control and Physical Audit, Rack Locking, and Environmental Monitoring.

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
September 1, 2023	August 31, 2028	5 - 12 Months	December 31, 2028
PAYMENT TERMS		DELIVERY TIMEFRAME	
n/a		n/a	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> Direct Voucher (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

n/a

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input type="checkbox"/>		<input type="checkbox"/>		
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$3,451,563.25	\$114,900.45	\$3,566,463.70		

DESCRIPTION

Effective 4/30/2025, this contract adds \$114,900.45 in funding to cover costs as described on the attached Statement of Work for the addition of the Nlyte Module, Audit at the amount of \$52,595.75. Additionally, this change notice adds the items listed at \$62,304.70 which were installed at the start of this Contract. The Audit Module is required to keep the data in sync between the Nlyte NEO and RFCODE and the addition of this \$114,900.45 will give the State the ability to purchase these items as needed.

All other terms, conditions, specifications and pricing remain the same. Per contractor and agency agreement, and DTMB Central Procurement Services approval.

STATEMENT OF WORK - IT CHANGE NOTICE

Quote No. JEMQ28481-01				
Part #	Qty.	Description	Unit Price	Ext. Price
PL/Rack	1	Perpetual License – Nlyte Audit – Rack – 560 Units	\$28,497.00	\$28,497.00
Support	1	Standard 8x5 Support and Maintenance until 12-31-2028	\$19,255.00	\$19,255.00
NPS	1	Nlyte Professional Services	\$4,843.75	\$4,843.75
			Subtotal:	\$52,595.75
			Tax:	\$0.00
			Shipping:	\$0.00
			Total:	\$52,595.75

Quote No. JEMQ28486-02				
Part #	Qty.	Description	Unit Price	Ext. Price
dbModularHandle	32	SwingHandle Latch Only – Interchangeable Modules	\$261.40	\$8,364.80
DB-CYL-003	32	DIN lock Plug with RS003 Key code	\$30.40	\$972.80
DBHC2KIT-SH	14	Smart Handle Conversion kit for horizontally mounted C2 latch	\$151.90	\$2,126.60
1000-S1389JB	14	Extended length cam w7mm offers used with the C2 horizontal kits	\$10.15	\$142.10
dbE5KIT-SH	14	Smart Handle Conversion Kit for EMC/Symmetrix 1 / 4 turn cabinets	\$151.90	\$2,126.60
dbSENTRY-KLKL(S)	8	Sentry w/2x CodeLock-HFLF (S), 2 door contacts – 1 CAT5e cable	\$2,268.35	\$18,146.80
Installation Services	100	Installation Services (Hourly Rate Includes all travel related expenses)	\$185.00	\$18,500.00
M174-iT05-000	500	IR-Enabled IT Asset Sensor Only	\$22.75	\$11,375.00
OTAB-i010	500	Flag Tag (4 inch)	\$1.10	\$550.00
			Subtotal:	\$62,304.70
			Tax:	\$0.00
			Shipping:	\$0.00
			Total:	\$62,304.70



STATE OF MICHIGAN
CENTRAL PROCUREMENT SERVICES
 Department of Technology, Management, and Budget
 320 S. WALNUT ST., LANSING, MICHIGAN 48933
 P.O. BOX 30026 LANSING, MICHIGAN 48909

CONTRACT CHANGE NOTICE

Change Notice Number 1
 to
 Contract Number 230000001430

CONTRACTOR	JEM TECH GROUP
	23537 Lakepointe Drive
	Clinton Twp, MI 48036
	Jami Moore
	586-783-3400
	j.moore@jemtechgroup.com
	CV0032887

STATE	Program Manager	Jennifer Poirier	DTMB
		517-242-2417	
	PoirierJ@Michigan.gov		
	Contract Administrator	Shannon Romein	DTMB
(517) 898-8102			
romeins@michigan.gov			

CONTRACT SUMMARY

HARDWARE AND SOFTWARE FOR THE ENTERPRISE OPERATIONS CENTER-DATA CENTER FOR VISITOR MANAGEMENT, ASSET CONTROL AND PHYSICAL AUDIT, RACK LOCKING, AND ENVIRONMENTAL MONITORING.

INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE
September 1, 2023	August 31, 2028	5 - 1 Year	August 31, 2028
PAYMENT TERMS		DELIVERY TIMEFRAME	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-Card <input type="checkbox"/> PRC <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

MINIMUM DELIVERY REQUIREMENTS

DESCRIPTION OF CHANGE NOTICE

OPTION	LENGTH OF OPTION	EXTENSION	LENGTH OF EXTENSION	REVISED EXP. DATE
<input checked="" type="checkbox"/>	4 months	<input type="checkbox"/>		December 31, 2028
CURRENT VALUE	VALUE OF CHANGE NOTICE	ESTIMATED AGGREGATE CONTRACT VALUE		
\$2,991,747.50	\$459,815.75	\$3,451,563.25		

DESCRIPTION

Effective 12/13/2023, four months of the five available option years are executed and the new Contract expiration date is 12/31/2028. Additionally, this Contract is hereby increased by \$459,815.75 and the following amendment is incorporated into the Contract for Neo and Nlyte maintenance and support costs through 12/31/2028.

All other terms, conditions, specifications, and pricing remain the same. Per contractor, agency, DTMB procurement and AD Board approval on 12/12/2023.



23537 Lakepointe Drive
 Clinton Township, MI 48036
 P: (586) 783-3400
 F: (586) 783-3430
 Email: support@jemtechgroup.com
 Web: www.jemtechgroup.com

Quote No. JEMQ26404
Date 11/17/2023

Company	Sales Representative	Quoted By
State of Michigan Jennifer Van Dyke	Jami Moore	Dave Lozon

Part #	Qty	Description	Unit Price	Ext. Price
Support Coverage Period is 01/01/2024 - 12/31/2028				
NEO Standard Support	5	NEO Standard Support: Support & Maintenance Standard (5 x 8) Nlyte Energy Optimizer 2500 Points	\$18,445.25	\$92,226.25
Support and Maintenance	5	Support & Maintenance Standard (5 x8): Nlyte Asset Optimizer 560 Racks	\$73,517.90	\$367,589.50
JEM MiDEAL Contract # 230000001430				

Comments:

Email: vandykej7@michigan.gov

SubTotal	\$459,815.75
Tax	\$0.00
Shipping	\$0.00
Total	\$459,815.75





STATE OF MICHIGAN PROCUREMENT
 Department of Technology, Management, and Budget
 320 S WALNUT ST, LANSING MI 48933
 PO BOX 30026, LANSING, MI 48909

NOTICE OF CONTRACT

NOTICE OF CONTRACT NO. **230000001430**
 between
 THE STATE OF MICHIGAN
 and

CONTRACTOR	JEM Computers, Inc. d/b/a JEM Tech Group
	23537 Lakepointe Drive
	Clinton Twp., MI 48036
	Jami Moore
	586-783-3400
	j.moore@jemtechgroup.com
	CV0032887

STATE	Program Manager	Jennifer Poirier	DTMB
		517-242-2417	
		poirierj@michigan.gov	
	Contract Administrator	Shannon Romein	DTMB
		517-898-8102	
		RomeinS@michigan.gov	

CONTRACT SUMMARY			
DESCRIPTION: Hardware and software for the Enterprise Operations Center-Data Center for Visitor Management, Asset Control and Physical Audit, Rack Locking, and Environmental Monitoring.			
INITIAL EFFECTIVE DATE	INITIAL EXPIRATION DATE	INITIAL AVAILABLE OPTIONS	EXPIRATION DATE BEFORE CHANGE(S) NOTED BELOW
September 1, 2023	August 31, 2028	5 – 1 year	August 31, 2028
PAYMENT TERMS		DELIVERY TIMEFRAME	
Net 45		N/A	
ALTERNATE PAYMENT OPTIONS			EXTENDED PURCHASING
<input type="checkbox"/> P-card <input type="checkbox"/> Payment Request (PRC) <input type="checkbox"/> Other			<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
MINIMUM DELIVERY REQUIREMENTS			
N/A			
MISCELLANEOUS INFORMATION			
This Contract is awarded from RFP # 220000002111			
ESTIMATED CONTRACT VALUE AT TIME OF EXECUTION			\$2,991,747.50

CONTRACT NO. 230000001430

FOR THE CONTRACTOR:

Company Name

Authorized Agent Signature

Authorized Agent (Print or Type)

Date

FOR THE STATE:

Signature

Name & Title

Agency

Date

STATE OF MICHIGAN

SOFTWARE TERMS AND CONDITIONS

These Terms and Conditions, together with all Schedules (including the Statement(s) of Work), Exhibits and any other applicable attachments or addenda (Collectively this “Contract”) are agreed to between the State of Michigan (the “**State**”) and JEM Computers, Inc. d/b/a JEM Tech Group (“**Contractor**”), a MICHIGAN CORPORATION. This Contract is effective on September 1, 2023] (“**Effective Date**”), and unless terminated, will expire on August 31, 2028] (the “**Term**”).

This Contract may be renewed for up to 5 additional 1-year period(s). Renewal is at the sole discretion of the State and will automatically extend the Term of this Contract. The State will document its exercise of renewal options via Contract Change Notice.

1. Definitions. For the purposes of this Contract, the following terms have the following meanings:

“**Acceptance**” has the meaning set forth in **Section 9**.

“**Acceptance Tests**” means such tests as may be conducted in accordance with **Section 9.1** and a Statement of Work to determine whether the Software meets the requirements of this Contract and the Documentation.

“**Affiliate**” of a Person means any other Person that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, such Person. For purposes of this definition, the term “control” (including the terms “controlled by” and “under common control with”) means the direct or indirect ownership of more than fifty percent (50%) of the voting securities of a Person.

“**Allegedly Infringing Materials**” has the meaning set forth in **Section 17.2(b)**.

“**Approved Third Party Components**” means all third party components, including Open-Source Components, that are included in or used in connection with the Software and are specifically identified by Contractor in the Contractor’s Bid Response or as part of the State’s Security Accreditation Process defined in Schedule E – Data Security Schedule.

“**Authorized Users**” means all Persons authorized by the State to access and use the Software under this Contract, subject to the maximum number of users specified in the applicable Statement of Work.

“**Business Day**” means a day other than a Saturday, Sunday or other day on which the State is authorized or required by law to be closed for business.

“**Business Requirements Specification**” means the initial specification setting forth the State’s business requirements regarding the features and functionality of the Software, as set forth in a Statement of Work.

“**Change**” has the meaning set forth in **Section 2.2**.

“**Change Notice**” has the meaning set forth in **Section 2.2(b)**.

“**Change Proposal**” has the meaning set forth in **Section 2.2(a)**.

“**Change Request**” has the meaning set forth in **Section 2.2**.

“**Confidential Information**” has the meaning set forth in **Section 22.1**.

“**Configuration**” means State-specific changes made to the Software without Source Code or structural data model changes occurring.

“**Contract**” has the meaning set forth in the preamble.

“**Contract Administrator**” is the individual appointed by each party to (a) administer the terms of this Contract, and (b) approve any Change Notices under this Contract. Each party’s Contract Administrator will be identified in a Statement of Work.

“**Contractor**” has the meaning set forth in the preamble.

“**Contractor’s Bid Response**” means the Contractor’s proposal submitted in response to the Solicitation Type.

“**Contractor Personnel**” means all employees of Contractor or any subcontractors or Permitted Subcontractors involved in the performance of Services hereunder.

“**Contractor Project Manager**” means the individual appointed by Contractor and identified in a Statement of Work to serve as the primary contact with regard to services, to monitor and coordinate the day-to-day activities of this Contract, and to perform other duties as may be further defined in this Contract, including an applicable Statement of Work.

“**Customization**” means State-specific changes to the Software’s underlying Source Code or structural data model changes.

“**Deliverables**” means the Software, Hardware, and all other documents and other materials that Contractor is required to or otherwise does provide to the State under this Contract and otherwise in connection with any Services, including all items specifically identified as Deliverables in a Statement of Work and all Work Product.

“**Deposit Material**” refers to material required to be deposited pursuant to **Section 28**.

“**Documentation**” means all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software or Hardware.

“**DTMB**” means the Michigan Department of Technology, Management and Budget.

“**Effective Date**” has the meaning set forth in the preamble.

“**Fees**” means the fees set forth in the Pricing Schedule attached as **Schedule B**.

“**Financial Audit Period**” has the meaning set forth in **Section 23.1**.

“**Hardware**” means all hardware provided by Contractor under this Contract, including but not limited to all hardware identified in a Statement of Work or Pricing Schedule and any related accessories.

“**Harmful Code**” means any software, hardware or other technologies, devices or means, the purpose or effect of which is to: (a) permit unauthorized access to, or to destroy, disrupt, disable, encrypt, modify, copy, or otherwise

harm or impede in any manner, any (i) computer, software, firmware, data, hardware, system or network, or (ii) any application or function of any of the foregoing or the integrity, use or operation of any data Processed thereby; or (b) prevent the State or any Authorized User from accessing or using the Services as intended by this Contract, and includes any virus, bug, trojan horse, worm, backdoor or other malicious computer code and any time bomb or drop dead device.

“**HIPAA**” has the meaning set forth in **Section 21.1**.

“**Hosted Services**” means the hosting, management and operation of the Operating Environment, Software, other services (including support and subcontracted services), and related resources for remote electronic access and use by the State and its Authorized Users, including any services and facilities related to disaster recovery obligations.

“**Implementation Plan**” means the schedule included in a Statement of Work setting forth the sequence of events for the performance of Services under a Statement of Work, including the Milestones and Milestone Dates.

“**Integration Testing**” has the meaning set forth in **Section 9.2(a)**.

“**Intellectual Property Rights**” means all or any of the following: (a) patents, patent disclosures, and inventions (whether patentable or not); (b) trademarks, service marks, trade dress, trade names, logos, corporate names, and domain names, together with all of the associated goodwill; (c) copyrights and copyrightable works (including computer programs), mask works and rights in data and databases; (d) trade secrets, know-how and other confidential information; and (e) all other intellectual property rights, in each case whether registered or unregistered and including all applications for, and renewals or extensions of, such rights, and all similar or equivalent rights or forms of protection provided by applicable law in any jurisdiction throughout the world.

“**Key Personnel**” means any Contractor Personnel identified as key personnel in the Contract.

“**License Agreements**” has the meaning set forth in **Section 5.1**.

“**Loss or Losses**” means all losses, including but not limited to, damages, liabilities, deficiencies, claims, actions, judgments, settlements, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees and the costs of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers.

“**Maintenance Release**” means any update, upgrade, release or other adaptation or modification of the Software, including any updated Documentation, that Contractor may generally provide to its licensees from time to time during the Term, which may contain, among other things, error corrections, enhancements, improvements or other changes to the user interface, functionality, compatibility, capabilities, performance, efficiency or quality of the Software.

“**Milestone**” means an event or task described in the Implementation Plan under a Statement of Work that must be completed by the corresponding Milestone Date.

“**Milestone Date**” means the date by which a particular Milestone must be completed as set forth in the Implementation Plan under a Statement of Work.

“**New Version**” means any new version of the Software, including any updated Documentation, that the Contractor may from time to time introduce and market generally as a distinct licensed product, as may be indicated by Contractor's designation of a new version number.

“Nonconformity” or **“Nonconformities”** means any failure or failures of the Software to conform to the requirements of this Contract, including any applicable Documentation.

“Open-Source Components” means any software component that is subject to any open-source copyright license agreement, including any GNU General Public License or GNU Library or Lesser Public License, or other obligation, restriction or license agreement that substantially conforms to the Open Source Definition as prescribed by the Open Source Initiative or otherwise may require disclosure or licensing to any third party of any source code with which such software component is used or compiled.

“Operating Environment” means, collectively, the platform, environment and conditions on, in or under which the Software is intended to be installed and operate, as set forth in a Statement of Work, including such structural, functional and other features, conditions and components as hardware, operating software, system architecture, configuration, computing hardware, ancillary equipment, networking, software, firmware, databases, data, and electronic systems (including database management systems).

“PAT” means a document or product accessibility template, including any Information Technology Industry Council Voluntary Product Accessibility Template or VPAT®, that specifies how information and software products, such as websites, applications, software and associated content, conform to WCAG 2.0 Level AA.

“Permitted Subcontractor” means any third party hired by Contractor or its Permitted Subcontractor to perform Services for the State under this Contract or have access to State Data.

“Person” means an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association or other entity.

“Pricing Schedule” means the schedule attached as **Schedule B**.

“Process” means to perform any operation or set of operations on any data, information, material, work, expression or other content, including to (a) collect, receive, input, upload, download, record, reproduce, store, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate or make other improvements or derivative works, (b) process, retrieve, output, consult, use, disseminate, transmit, submit, post, transfer, disclose or otherwise provide or make available, or (c) block, erase or destroy. **“Processing”** and **“Processed”** have correlative meanings.

“Representatives” means a party's employees, officers, directors, partners, shareholders, agents, attorneys, successors and permitted assigns.

“RFP” means the State's request for proposal designed to solicit responses for Services under this Contract.

“Services” means any of the services, including but not limited to, Hosted Services, Contractor is required to or otherwise does provide under this Contract.

“Service Level Agreement” means the schedule attached as **Schedule D**, setting forth the Support Services Contractor will provide to the State, and the parties' additional rights and obligations with respect thereto.

“Site” means the physical location designated by the State in, or in accordance with, this Contract or a Statement of Work for delivery and installation of the Software or Hardware, as applicable.

“Software” means all software provided by Contractor under this Contract, including but not limited to Contractor's software, third party software, any Maintenance Releases or New Versions provided to the State and

any Customizations or Configurations made by or for the State pursuant to this Contract, and all copies of the foregoing permitted under this Contract and the License Agreements.

“**Source Code**” means the human readable source code of the Software to which it relates, in the programming language in which the Software was written, together with all related flow charts and technical documentation, including a description of the procedure for generating object code, all of a level sufficient to enable a programmer reasonably fluent in such programming language to understand, build, operate, support, maintain and develop modifications, upgrades, updates, adaptations, enhancements, new versions and other derivative works and improvements of, and to develop computer programs compatible with, the Software.

“**Specifications**” means, for the Software, the specifications collectively set forth in the Business Requirements Specification, Technical Specification, Documentation, Request for Proposal or Contractor’s Bid Response, if any, for such Software, or elsewhere in a Statement of Work.

“**State**” means the State of Michigan.

“**State Data**” has the meaning set forth in **Section 21.1**.

“**State Hosted**” means the Hosted Services are not provided by Contractor or one or more of its Permitted Subcontractors.

“**State Materials**” means all materials and information, including documents, data, know-how, ideas, methodologies, specifications, software, hardware, content and technology, in any form or media, directly or indirectly provided or made available to Contractor by or on behalf of the State in connection with this Contract.

“**State Program Managers**” are the individuals appointed by the State, or their designees, to (a) monitor and coordinate the day-to-day activities of this Contract; (b) co-sign off on Acceptance of the Software and other Deliverables; and (c) perform other duties as may be specified in a Statement of Work Program Managers will be identified in a Statement of Work.

“**State Systems**” means the information technology infrastructure, including the computers, software, databases, electronic systems (including database management systems) and networks, of the State or any of its designees.

“**Statement of Work**” means any statement of work entered into by the parties and incorporated into this Contract. The initial Statement of Work is attached as **Schedule A**.

“**Stop Work Order**” has the meaning set forth in **Section 15**.

“**Support Services**” means the software maintenance and support services Contractor is required to or otherwise does provide to the State under the Service Level Agreement.

“**Technical Specification**” means, with respect to any Software, the document setting forth the technical specifications for such Software and included in a Statement of Work.

“**Term**” has the meaning set forth in the preamble.

“**Testing Period**” has the meaning set forth in **Section 9.1(b)**.

“**Transition Period**” has the meaning set forth in **Section 16.3**.

“**Transition Responsibilities**” has the meaning set forth in **Section 16.3**.

“**Unauthorized Removal**” has the meaning set forth in **Section 2.5(b)**.

“**Unauthorized Removal Credit**” has the meaning set forth in **Section 2.5(c)**.

“**User Data**” means all data, information and other content of any type and in any format, medium or form, whether audio, visual, digital, screen, GUI or other, that is input, uploaded to, placed into or collected, stored, Processed, generated or output by any device, system or network by or on behalf of the State, including any and all works, inventions, data, analyses and other information and materials resulting from any use of the Software by or on behalf of the State under this Contract, except that User Data does not include the Software or data, information or content, including any GUI, audio, visual or digital or other display or output, that is generated automatically upon executing the Software without additional user input without the inclusion of user derived Information or additional user input.

“**Warranty Period**” means the ninety (90) calendar-day period commencing on the date of the State's Acceptance of the Software and Hardware and for which Support Services are provided free of charge.

“**WCAG 2.0 Level AA**” means level AA of the World Wide Web Consortium Web Content Accessibility Guidelines version 2.0.

“**Work Product**” means all State-specific deliverables that Contractor is required to, or otherwise does, provide to the State under this Contract including but not limited to Customizations, application programming interfaces, computer scripts, macros, user interfaces, reports, project management documents, forms, templates, and other State-specific documents and related materials together with all ideas, concepts, processes, and methodologies developed in connection with this Contract whether or not embodied in this Contract.

2. Duties of Contractor. Contractor will provide Services and Deliverables pursuant to Statement(s) of Work entered into under this Contract. Contractor will provide all Services and Deliverables in a timely, professional manner and in accordance with the terms, conditions, and Specifications set forth in this Contract and the Statement(s) of Work.

2.1 Statement of Work Requirements. No Statement of Work will be effective unless signed by each party's Contract Administrator. The term of each Statement of Work will commence on the parties' full execution of a Statement of Work and terminate when the parties have fully performed their obligations. The terms and conditions of this Contract will apply at all times to any Statements of Work entered into by the parties and incorporated into this Contract. The State will have the right to terminate such Statement of Work as set forth in **Section 16**. Contractor acknowledges that time is of the essence with respect to Contractor's obligations under each Statement of Work and agrees that prompt and timely performance of all such obligations in accordance with this Contract and the Statements of Work (including the Implementation Plan and all Milestone Dates) is strictly required.

2.2 Change Control Process. The State may at any time request in writing (each, a “**Change Request**”) changes to a Statement of Work, including changes to the Services and Implementation Plan (each, a “**Change**”). Upon the State's submission of a Change Request, the parties will evaluate and implement all Changes in accordance with this **Section 2.2**.

(a) As soon as reasonably practicable, and in any case within twenty (20) Business Days following receipt of a Change Request, Contractor will provide the State with a written proposal for implementing the requested Change (“**Change Proposal**”), setting forth:

- (i) a written description of the proposed Changes to any Services or Deliverables;

- (ii) an amended Implementation Plan reflecting: (A) the schedule for commencing and completing any additional or modified Services or Deliverables; and (B) the effect of such Changes, if any, on completing any other Services under a Statement of Work;
- (iii) any additional State Resources Contractor deems necessary to carry out such Changes; and
- (iv) any increase or decrease in Fees resulting from the proposed Changes, which increase or decrease will reflect only the increase or decrease in time and expenses Contractor requires to carry out the Change.

(b) Within thirty (30) Business Days following the State's receipt of a Change Proposal, the State will by written notice to Contractor, approve, reject, or propose modifications to such Change Proposal. If the State proposes modifications, Contractor must modify and re-deliver the Change Proposal reflecting such modifications, or notify the State of any disagreement, in which event the parties will negotiate in good faith to resolve their disagreement. Upon the State's approval of the Change Proposal or the parties' agreement on all proposed modifications, as the case may be, the parties will execute a written agreement to the Change Proposal ("**Change Notice**"), which Change Notice will be signed by the State's Contract Administrator and will constitute an amendment to a Statement of Work to which it relates; and

(c) If the parties fail to enter into a Change Notice within fifteen (15) Business Days following the State's response to a Change Proposal, the State may, in its discretion:

- (i) require Contractor to perform the Services under a Statement of Work without the Change;
- (ii) require Contractor to continue to negotiate a Change Notice;
- (iii) initiate a Dispute Resolution Procedure; or
- (iv) notwithstanding any provision to the contrary in a Statement of Work, terminate this Contract under **Section 16.1**.

(d) No Change will be effective until the parties have executed a Change Notice. Except as the State may request in its Change Request or otherwise in writing, Contractor must continue to perform its obligations in accordance with a Statement of Work pending negotiation and execution of a Change Notice. Contractor will use its best efforts to limit any delays or Fee increases from any Change to those necessary to perform the Change in accordance with the applicable Change Notice. Each party is responsible for its own costs and expenses of preparing, evaluating, negotiating, and otherwise processing any Change Request, Change Proposal, and Change Notice.

(e) The performance of any functions, activities, tasks, obligations, roles and responsibilities comprising the Services as described in this Contract are considered part of the Services and, thus, will not be considered a Change. This includes the delivery of all Deliverables in accordance with their respective Specifications, and the diagnosis and correction of Non-Conformities discovered in Deliverables prior to their Acceptance by the State or, subsequent to their Acceptance by the State, as necessary for Contractor to fulfill its associated warranty requirements and its Support Services under this Contract.

(f) Contractor may, on its own initiative and at its own expense, prepare and submit its own Change Request to the State. However, the State will be under no obligation to approve or otherwise respond to a Change Request initiated by Contractor.

2.3 Contractor Personnel.

(a) Contractor is solely responsible for all Contractor Personnel and for the payment of their compensation, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits.

(b) Prior to any Contractor Personnel performing any Services, Contractor will:

- (i) ensure that such Contractor Personnel have the legal right to work in the United States;
- (ii) upon request, require such Contractor Personnel to execute written agreements, in form and substance acceptable to the State, that bind such Contractor Personnel to confidentiality provisions that are at least as protective of the State's information (including all Confidential Information) as those contained in this Contract; and
- (iii) upon request, or as otherwise specified in a Statement of Work, perform background checks on all Contractor Personnel prior to their assignment. The scope is at the discretion of the State and documentation must be provided as requested. Contractor is responsible for all costs associated with the requested background checks. The State, in its sole discretion, may also perform background checks on Contractor Personnel. Pursuant to Michigan law, all agencies subject to IRS Pub. 1075 are required to ask the Michigan State Police to perform fingerprint background checks on all employees, including Contractor and subcontractor employees, who may have access to any database of information maintained by the federal government that contains confidential or personal information, including, but not limited to, federal tax information. Further, pursuant to Michigan law, any agency described above is prohibited from providing Contractors or subcontractors with the result of such background check. For more information, please see Michigan Public Act 427 of 2018.

(c) Contractor and all Contractor Personnel will comply with all rules, regulations, and policies of the State that are communicated to Contractor in writing, including security procedures concerning systems and data and remote access, building security procedures, including the restriction of access by the State to certain areas of its premises or systems, and general health and safety practices and procedures.

(d) The State reserves the right to require the removal of any Contractor Personnel found, in the judgment of the State, to be unacceptable. The State's request must be written with reasonable detail outlining the reasons for the removal request. Replacement personnel for the removed person must be fully qualified for the position. If the State exercises this right, and Contractor cannot immediately replace the removed personnel, the State agrees to negotiate an equitable adjustment in schedule or other terms that may be affected by the State's required removal.

2.4 Contractor Project Manager. Throughout the Term of this Contract, Contractor must maintain a Contractor employee acceptable to the State to serve as Contractor Project Manager, who will be considered Key Personnel of Contractor. Contractor Project Manager will be identified in a Statement of Work.

(a) Contractor Project Manager must:

- (i) have the requisite authority, and necessary skill, experience, and qualifications, to perform in such capacity;
- (ii) be responsible for overall management and supervision of Contractor's performance under this Contract; and

- (iii) be the State's primary point of contact for communications with respect to this Contract, including with respect to giving and receiving all day-to-day approvals and consents.
- (b) Contractor Project Manager must attend all regularly scheduled meetings as set forth in the Implementation Plan and will otherwise be available as set forth in a Statement of Work.
- (c) Contractor will maintain the same Contractor Project Manager throughout the Term of this Contract, unless:
 - (i) the State requests in writing the removal of Contractor Project Manager;
 - (ii) the State consents in writing to any removal requested by Contractor in writing;
 - (iii) Contractor Project Manager ceases to be employed by Contractor, whether by resignation, involuntary termination or otherwise.
- (d) Contractor will promptly replace its Contractor Project Manager on the occurrence of any event set forth in **Section 2.4(c)**. Such replacement will be subject to the State's prior written approval.

2.5 Contractor's Key Personnel.

(a) The State has the right to recommend and approve in writing the initial assignment, as well as any proposed reassignment or replacement, of any Key Personnel. Before assigning an individual to any Key Personnel position, Contractor will notify the State of the proposed assignment, introduce the individual to the State Program Managers or their designees, and provide the State with a resume and any other information about the individual reasonably requested by the State. The State reserves the right to interview the individual before granting written approval. In the event the State finds a proposed individual unacceptable, the State will provide a written explanation including reasonable detail outlining the reasons for the rejection.

(b) Contractor will not remove any Key Personnel from their assigned roles on this Contract without the prior written consent of the State. The Contractor's removal of Key Personnel without the prior written consent of the State is an unauthorized removal ("**Unauthorized Removal**"). An Unauthorized Removal does not include replacing Key Personnel for reasons beyond the reasonable control of Contractor, including illness, disability, leave of absence, personal emergency circumstances, resignation, or for cause termination of the Key Personnel's employment. Any Unauthorized Removal may be considered by the State to be a material breach of this Contract, in respect of which the State may elect to terminate this Contract for cause under **Section 16.1**.

(c) It is further acknowledged that an Unauthorized Removal will interfere with the timely and proper completion of this Contract, to the loss and damage of the State, and that it would be impracticable and extremely difficult to determine and remedy the actual damage sustained by the State as a result of any Unauthorized Removal. Therefore, Contractor and the State agree that in the case of any Unauthorized Removal in respect of which the State does not elect to exercise its rights under **Section 16**, Contractor will issue to the State an amount equal to \$25,000 per individual (each, an "**Unauthorized Removal Credit**").

(d) Contractor acknowledges and agrees that each of the Unauthorized Removal Credits assessed under **Subsection 2.5(c)** above: (i) is a reasonable estimate of and compensation for the anticipated or actual harm to the State that may arise from the Unauthorized Removal, which would be impossible or very difficult to accurately estimate; and (ii) may, at the State's option, be credited or set off against any Fees or other charges payable to Contractor under this Contract.

2.6 Subcontractors. Contractor must obtain prior written approval of the State, which consent may be given or withheld in the State's sole discretion, before engaging any Permitted Subcontractor to provide Services to the State

under this Contract. Third parties otherwise retained by Contractor to provide Contractor or other clients of contractor with services are not Permitted Subcontractors, and therefore do not require prior approval by the State. Engagement of any subcontractor or Permitted Subcontractor by Contractor does not relieve Contractor of its representations, warranties or obligations under this Contract. Without limiting the foregoing, Contractor will:

(a) be responsible and liable for the acts and omissions of each such subcontractor (including such Permitted Subcontractor and Permitted Subcontractor's employees who, to the extent providing Services or Deliverables, will be deemed Contractor Personnel) to the same extent as if such acts or omissions were by Contractor or its employees;

(b) Reserved;

(c) be responsible for all fees and expenses payable to, by or on behalf of each Permitted Subcontractor in connection with this Contract, including, if applicable, withholding of income taxes, and the payment and withholding of social security and other payroll taxes, unemployment insurance, workers' compensation insurance payments and disability benefits; and

(d) notify the State of the location of the Permitted Subcontractor and indicate if it is located within the continental United States.

3. Notices. All notices and other communications required or permitted under this Contract must be in writing and will be considered given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email.

If to State: Shannon Romein 320 S Walnut St #6 Lansing, MI 48933 Romeins@michigan.gov 517-898-8102	If to Contractor: Jami Moore 23537 Lakepointe Dr Clinton Twp., MI 48036 j.moore@jemtechgroup.com 586-783-3400
--	---

4. Insurance. Contractor must maintain the minimum insurances identified in the Insurance Schedule attached as **Schedule C**.

5. Licenses. For purposes of this **Section 5**, the term "Software" does not include Customizations.

5.1 Software License Agreement. The State and its Authorized Users' rights to use the Software and Documentation are set forth in this Section 5.1, and where applicable, in license terms set forth in Schedule I (collectively, the "**License Agreements**")

(a) **Contractor License Grant to State.** If Contractor is granting a license to any Software under this Contract, Contractor hereby grants to the State and its Authorized Users a non-exclusive, royalty-free, perpetual, irrevocable right and license to use the Software and Documentation in accordance with the terms and conditions of this Contract, provided that:

- (i) The State is prohibited from reverse engineering or decompiling the Software, making derivative works, modifying, adapting or copying the Software except as is expressly permitted by this Contract or required to be permitted by law;
- (ii) The State is authorized to make copies of the Software for backup, disaster recovery, and archival purposes;

- (iii) The State is authorized to make copies of the Software to establish a test environment to conduct Acceptance Testing;
- (iv) Title to and ownership of the Software shall at all times remain with Contractor and/or its licensors, as applicable; and
- (v) Except as expressly agreed in writing, the State is not permitted to sub-license the use of the Software or any accompanying Documentation.

(b) **Certification.** Unless otherwise agreed in a License Agreement, to the extent that a License granted to the State is not unlimited, Contractor may request written certification from the State regarding use of the Software for the sole purpose of verifying compliance with this **Section 5.1**. Such written certification may occur no more than once in any twenty four (24) month period during the Term of the Contract. The State will respond to any such request within 45 calendar days of receipt. If the State's use is greater than contracted, Contractor may invoice the State for any unlicensed use (and related support) pursuant to the terms of this Contract at the rates set forth in **Schedule B**, and the unpaid license and support fees shall be payable in accordance with the terms of the Contract. Payment under this provision shall be Contractor's sole and exclusive remedy to cure these issues.

5.2 State License Grant to Contractor. The State hereby grants to Contractor a limited, non-exclusive, non-transferable license (i) to use the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos, solely in accordance with the State's specifications, and (ii) to display, reproduce, distribute and transmit in digital form the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos in connection with promotion of the Services as communicated to Contractor by the State. Use of the State's (or individual agency's, department's or division's) name, trademarks, service marks or logos will be specified in the applicable Statement of Work. Contractor is provided a limited license to State Materials for the sole and exclusive purpose of providing the Services.

6. Third Party Components. At least 30 days prior to adding new Approved Third Party Components, Contractor will provide the State with notification information identifying and describing the addition. Throughout the Term, on an annual basis, Contractor will provide updated information identifying and describing any Approved Third Party Components included in the Software.

7. Intellectual Property Rights

7.1 Ownership Rights in Software

- (a) For purposes of this **Section 7** only, the term "Software" does not include Customizations.
- (b) Subject to the rights and licenses granted by Contractor in this Contract and the provisions of **Section**

7.1(c):

- (i) Contractor reserves and retains its entire right, title and interest in and to all Intellectual Property Rights arising out of or relating to the Software, if any; and
- (ii) none of the State or Authorized Users acquire any ownership of Intellectual Property Rights in or to the Software or Documentation as a result of this Contract.

(c) As between the State, on the one hand, and Contractor, on the other hand, the State has, reserves and retains, sole and exclusive ownership of all right, title and interest in and to State Materials and User Data, including all Intellectual Property Rights arising therefrom or relating thereto.

7.2 The State is and will be the sole and exclusive owner of all right, title, and interest in and to all Work Product developed exclusively for the State under this Contract, including all Intellectual Property Rights. In furtherance of the foregoing:

(a) Contractor will create all Work Product as work made for hire as defined in Section 101 of the Copyright Act of 1976; and

(b) to the extent any Work Product, or Intellectual Property Rights do not qualify as, or otherwise fails to be, work made for hire, Contractor hereby:

- (i) assigns, transfers, and otherwise conveys to the State, irrevocably and in perpetuity, throughout the universe, all right, title, and interest in and to such Work Product, including all Intellectual Property Rights; and
- (ii) irrevocably waives any and all claims Contractor may now or hereafter have in any jurisdiction to so-called "moral rights" or rights of *droit moral* with respect to the Work Product.

8. Software Implementation.

8.1 Implementation. Contractor will as applicable; deliver, install, configure, integrate, and otherwise provide and make fully operational the Software on or prior to the applicable Milestone Date in accordance with the criteria set forth in a Statement of Work and the Implementation Plan.

8.2 Site Preparation. Unless otherwise set forth in a Statement of Work, Contractor is responsible for ensuring the relevant Operating Environment is set up and in working order to allow Contractor to deliver and install the Software on or prior to the applicable Milestone Date. Contractor will provide the State with such notice as is specified in a Statement of Work, prior to delivery of the Software to give the State sufficient time to prepare for Contractor's delivery and installation of the Software. If the State is responsible for Site preparation, Contractor will provide such assistance as the State requests to complete such preparation on a timely basis.

9. Software Acceptance Testing.

9.1 Software Acceptance Testing.

(a) Unless otherwise specified in a Statement of Work, upon installation of the Software, Acceptance Tests will be conducted as set forth in this **Section 9** to ensure the Software conforms to the requirements of this Contract, including the applicable Specifications and Documentation.

(b) All Acceptance Tests will take place at the designated Site(s) in the Operating Environment described in a Statement of Work, commence on the Business Day following installation of the Software, or the receipt by the State of the notification in **Section 9.1(a)**, and be conducted diligently for up to thirty (30) Business Days, or such other period as may be set forth in a Statement of Work (the "**Testing Period**"). Acceptance Tests will be conducted by the party responsible as set forth in a Statement of Work or, if a Statement of Work does not specify, the State, provided that:

- (i) for Acceptance Tests conducted by the State, if requested by the State, Contractor will make suitable Contractor Personnel available to observe or participate in such Acceptance Tests; and
- (ii) for Acceptance Tests conducted by Contractor, the State has the right to observe or participate in all or any part of such Acceptance Tests.

9.2 Contractor is solely responsible for all costs and expenses related to Contractor's performance of, participation in, and observation of Acceptance Testing.

(a) Upon delivery and installation of any application programming interfaces, Configuration or Customizations, or any other applicable Work Product, to the Software under a Statement of Work, additional Acceptance Tests will be performed on the modified Software as a whole to ensure full operability, integration, and compatibility among all elements of the Software ("**Integration Testing**"). Integration Testing is subject to all procedural and other terms and conditions set forth in **Section 9.1**, **Section 9.4**, and **Section 9.5**.

(b) The State may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if the State discovers a material Non-Conformity in the tested Software or part or feature of the Software. In such event, Contractor will immediately, and in any case within ten (10) Business Days, correct such Non-Conformity, whereupon the Acceptance Tests and Testing Period will resume for the balance of the Testing Period.

9.3 Notices of Completion, Non-Conformities, and Acceptance. Within fifteen (15) Business Days following the completion of any Acceptance Tests, including any Integration Testing, the party responsible for conducting the tests will prepare and provide to the other party written notice of the completion of the tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Non-Conformity in the tested Software.

(a) If such notice is provided by either party and identifies any Non-Conformities, the parties' rights, remedies, and obligations will be as set forth in **Section 9.4** and **Section 9.5**.

(b) If such notice is provided by the State, is signed by the State Program Managers or their designees, and identifies no Non-Conformities, such notice constitutes the State's Acceptance of such Software.

(c) If such notice is provided by Contractor and identifies no Non-Conformities, the State will have thirty (30) Business Days to use the Software in the Operating Environment and determine, in the exercise of its sole discretion, whether it is satisfied that the Software contains no Non-Conformities, on the completion of which the State will, as appropriate:

- (i) notify Contractor in writing of Non-Conformities the State has observed in the Software and of the State's non-acceptance thereof, whereupon the parties' rights, remedies and obligations will be as set forth in **Section 9.4** and **Section 9.5**; or
- (ii) provide Contractor with a written notice of its Acceptance of such Software, which must be signed by the State Program Managers or their designees.

9.4 Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformities, Contractor, at Contractor's sole cost and expense, will remedy all such Non-Conformities and re-deliver the Software, in accordance with the requirements set forth in a Statement of Work. Redelivery will occur as promptly as commercially possible and, in any case, within thirty (30) Business Days following, as applicable, Contractor's:

- (a) completion of such Acceptance Tests, in the case of Acceptance Tests conducted by Contractor; or
- (b) receipt of the State's notice under **Section 9.1(a)** or **Section 9.3(c)(i)**, identifying any Non-Conformities.

9.5 Repeated Failure of Acceptance Tests. If Acceptance Tests identify any Non-Conformity in the Software after a second or subsequent delivery of the Software, or Contractor fails to re-deliver the Software on a timely basis, the State may, in its sole discretion, by written notice to Contractor:

(a) continue the process set forth in this **Section 9**;

(b) accept the Software as a nonconforming deliverable, in which case the Fees for such Software will be reduced equitably to reflect the value of the Software as received relative to the value of the Software had it conformed; or

(c) deem the failure to be a non-curable material breach of this Contract and a Statement of Work and terminate this Contract for cause in accordance with **Section 16.1**.

9.6 Acceptance. Acceptance (“**Acceptance**”) of the Software (subject, where applicable, to the State’s right to Integration Testing) and any Deliverables will occur on the date that is the earliest of the State’s delivery of a notice accepting the Software or Deliverables under **Section 9.3(b)**, or **Section 9.3(c)(ii)**.

10. Non-Software Acceptance.

10.1 Delivery, Acceptance and Warranty of Hardware. Requirements for delivery, acceptance and warranty of Hardware are set forth in **Schedule G**.

10.2 Acceptance of the System. Requirements for User Acceptance Testing (UAT) of the Software and Hardware, as an integrated system, are set forth in **Schedule H**.

10.3 All other Services and Deliverables not addressed in Sections 9, 10.1 and 10.2 (“Other Deliverables”) are subject to inspection and testing by the State within 30 calendar days of the State’s receipt of them (“State Review Period”), unless otherwise provided in the Statement of Work. If the Other Deliverables are not fully accepted by the State, the State will notify Contractor by the end of the State Review Period that either: (a) the Other Deliverables are accepted but noted deficiencies must be corrected; or (b) the Other Deliverables are rejected. If the State finds material deficiencies, it may: (i) reject the Other Deliverables without performing any further inspections; (ii) demand performance at no additional cost; or (iii) terminate this Contract in accordance with **Section 16.1**, Termination for Cause.

(a) Within 10 business days from the date of Contractor’s receipt of notification of acceptance with deficiencies or rejection of any Other Deliverables, Contractor must cure, at no additional cost, the deficiency and deliver unequivocally acceptable Other Deliverables to the State. If acceptance with deficiencies or rejection of the Other Deliverables impacts the content or delivery of other non-completed Other Deliverables, the parties’ respective Program Managers must determine an agreed to number of days for re-submission that minimizes the overall impact to the Contract. However, nothing herein affects, alters, or relieves Contractor of its obligations to correct deficiencies in accordance with the time response standards set forth in this Contract.

(b) If Contractor is unable or refuses to correct the deficiency within the time response standards set forth in this Contract, the State may cancel the order in whole or in part. The State, or a third party identified by the State, may provide the non-Software Services and Deliverables and recover the difference between the cost to cure and the Contract price plus an additional 10% administrative fee.

11. Assignment. Contractor may not assign this Contract to any other party without the prior approval of the State. Upon notice to Contractor, the State, in its sole discretion, may assign in whole or in part, its rights or responsibilities under this Contract to any other party. If the State determines that a novation of the Contract to a third party is necessary, Contractor will agree to the novation and provide all necessary documentation and signatures.

12. Change of Control. Contractor will notify the State, within 30 days of any public announcement or otherwise once legally permitted to do so, of a change in Contractor’s organizational structure or ownership. For purposes of this Contract, a change in control means any of the following:

- (a) a sale of more than 50% of Contractor's stock;
- (b) a sale of substantially all of Contractor's assets;
- (c) a change in a majority of Contractor's board members;
- (d) consummation of a merger or consolidation of Contractor with any other entity;
- (e) a change in ownership through a transaction or series of transactions;
- (f) or the board (or the stockholders) approves a plan of complete liquidation.

A change of control does not include any consolidation or merger effected exclusively to change the domicile of Contractor, or any transaction or series of transactions principally for bona fide equity financing purposes. In the event of a change of control, Contractor must require the successor to assume this Contract and all of its obligations under this Contract.

13. Invoices and Payment.

13.1 Invoices must conform to the requirements communicated from time-to-time by the State. All undisputed amounts are payable within 45 days of the State's receipt. Contractor may only charge for Services and Deliverables provided as specified in Statement(s) of Work. Invoices must include an itemized statement of all charges.

13.2 The State has the right to withhold payment of any disputed amounts until the parties agree as to the validity of the disputed amount. The State will notify Contractor of any dispute within a reasonable time. Payment by the State will not constitute a waiver of any rights as to Contractor's continuing obligations, including claims for deficiencies or substandard Services and Deliverables. Contractor's acceptance of final payment by the State constitutes a waiver of all claims by Contractor against the State for payment under this Contract, other than those claims previously filed in writing on a timely basis and still disputed.

13.3 The State will only disburse payments under this Contract through Electronic Funds Transfer (EFT). Contractor must register with the State at <http://www.michigan.gov/SIGMAVSS> to receive electronic fund transfer payments. If Contractor does not register, the State is not liable for failure to provide payment.

13.4 Right of Setoff. Without prejudice to any other right or remedy it may have, the State reserves the right to set off at any time any amount then due and owing to it by Contractor against any amount payable by the State to Contractor under this Contract.

13.5 Taxes. The State is exempt from State sales tax for direct purchases and may be exempt from federal excise tax, if Services or Deliverables purchased under this Contract are for the State's exclusive use. Notwithstanding the foregoing, all Fees are exclusive of taxes, and Contractor is responsible for all sales, use and excise taxes, and any other similar taxes, duties and charges of any kind imposed by any federal, state, or local governmental entity on any amounts payable by the State under this Contract.

13.6 Pricing/Fee Changes. All Pricing set forth in this Contract will not be increased, except as otherwise expressly provided in this Section.

(a) The Fees will not be increased at any time except for the addition of additional licenses, the fees for which licenses will also remain firm in accordance with the Pricing set forth in the Pricing Schedule.

(b) Excluding federal government charges and terms. Contractor warrants and agrees that each of the Fees, economic or product terms or warranties granted pursuant to this Contract are comparable to or better than the equivalent fees, economic or product term or warranty being offered to any commercial or government customer of

Contractor. If Contractor enters into any arrangements with another customer of Contractor to provide the products or services, available under this Contract, under more favorable prices, as the prices may be indicated on Contractor's current U.S. and International price list or comparable document, then this Contract will be deemed amended as of the date of such other arrangements to incorporate those more favorable prices, and Contractor will immediately notify the State of such Fee and formally memorialize the new pricing in a Change Notice.

13.7 Provided the State has made its payments to Contractor for Deliverables and/or Services pursuant to the terms of this Contract, Contractor's failure to pay any of its subcontractors or suppliers (including without limitation third-party manufacturers, software publishers, or other suppliers of products and/or services under this Contract) will constitute a material breach of this Contract. Contractor will be responsible for any and all damages resulting from its failure to pay its subcontractors and/or suppliers and any such damages are considered to be direct damages.

14. Liquidated Damages.

14.1 The parties understand and agree that any liquidated damages (which includes but is not limited to applicable credits) set forth in this Contract are reasonable estimates of the State's damages in accordance with applicable law.

14.2 The parties acknowledge and agree that Contractor could incur liquidated damages for more than one event.

14.3 The assessment of liquidated damages will not constitute a waiver or release of any other remedy the State may have under this Contract for Contractor's breach of this Contract, including without limitation, the State's right to terminate this Contract for cause under **Section 16.1** and the State will be entitled in its discretion to recover actual damages caused by Contractor's failure to perform its obligations under this Contract. However, the State will reduce such actual damages by the amounts of liquidated damages received for the same events causing the actual damages.

14.4 Amounts due the State as liquidated damages may be set off against any Fees payable to Contractor under this Contract, or the State may bill Contractor as a separate item and Contractor will promptly make payments on such bills.

15. Stop Work Order. The State may, at any time, order the Services of Contractor fully or partially stopped for up to ninety (90) calendar days at no additional cost to the State. The State will provide Contractor a written notice detailing such suspension (a "**Stop Work Order**"). Contractor must comply with the Stop Work Order upon receipt. Within 90 days, or any longer period agreed to by Contractor, the State will either:

(a) issue a notice authorizing Contractor to resume work, or

(b) terminate this Contract. The State will not pay for any Services, Contractor's lost profits, or any additional compensation during a stop work period.

16. Termination, Expiration, Transition. The State may terminate this Contract, the Support Services, or any Statement of Work, in accordance with the following:

16.1 Termination for Cause. In addition to any right of termination set forth elsewhere in this Contract:

(a) The State may terminate this Contract for cause, in whole or in part, if Contractor, as determined by the State:

(i) endangers the value, integrity, or security of State Systems, State Data, or the State's facilities or personnel;

- (ii) becomes insolvent, petitions for bankruptcy court proceedings, or has an involuntary bankruptcy proceeding filed against it by any creditor; or
- (iii) breaches any of its material duties or obligations under this Contract. Any reference to specific breaches being material breaches within this Contract will not be construed to mean that other breaches are not material.

(b) If the State terminates this Contract under this **Section 16.1**, the State will issue a termination notice specifying whether Contractor must:

- (i) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or
- (ii) continue to perform for a specified period. If it is later determined that Contractor was not in breach of this Contract, the termination will be deemed to have been a termination for public interest, effective as of the same date, and the rights and obligations of the parties will be limited to those provided in **Section 16.2**.

(c) The State will only pay for amounts due to Contractor for Services accepted by the State on or before the date of termination, subject to the State's right to set off any amounts owed by the Contractor for the State's reasonable costs in terminating this Contract. Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination, including any prepaid Fees. Further, Contractor must pay all reasonable costs incurred by the State in terminating this Contract for cause, including administrative costs, attorneys' fees, court costs, transition costs, and any costs the State incurs to procure the Services from other sources.

16.2 Termination for Public Interest. The State may immediately terminate this Contract in whole or in part, without penalty and for any reason, including but not limited to, appropriation or budget shortfalls. The termination notice will specify whether Contractor must:

(a) cease performance immediately. Contractor must submit all invoices for Services accepted by the State within 30 days of the date of termination. Failure to submit an invoice within that timeframe will constitute a waiver by Contractor for any amounts due to Contractor for Services accepted by the State under this Contract, or

(b) continue to perform in accordance with **Section 16.3**. If the State terminates this Contract for public interest, the State will pay all reasonable costs, as determined by the State, for State approved Transition Responsibilities to the extent the funds are available.

16.3 Transition Responsibilities.

(a) Upon termination or expiration of this Contract for any reason, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days; the "**Transition Period**"), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the Contract to continue without interruption or adverse effect, and to facilitate the orderly transfer of the Services to the State or its designees. Such transition assistance may include but is not limited to:

- (i) continuing to perform the Services at the established Contract rates;
- (ii) taking all reasonable and necessary measures to transition performance of the work, including all applicable Services to the State or the State's designee;

- (iii) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, and comply with **Section 22.5** regarding the return or destruction of State Data at the conclusion of the Transition Period; and
- (iv) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts (collectively, the “**Transition Responsibilities**”). The Term of this Contract is automatically extended through the end of the Transition Period.

(b) Contractor will follow the transition plan attached as **Schedule F** as it pertains to both transition in and transition out activities.

17. Indemnification

17.1 General Indemnification. Contractor must defend, indemnify and hold the State, its departments, divisions, agencies, offices, commissions, officers, and employees harmless, without limitation, from and against any and all actions, claims, losses, liabilities, damages, costs, attorney fees, and expenses (including those required to establish the right to indemnification), arising out of or relating to:

(a) any breach by Contractor (or any of Contractor’s employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable) of any of the promises, agreements, representations, warranties, or insurance requirements contained in this Contract;

(b) any infringement, misappropriation, or other violation of any Intellectual Property Right or other right of any third party;

(c) any bodily injury, death, or damage to real or tangible personal property occurring wholly or in part due to action or inaction by Contractor (or any of Contractor’s employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable); and

(d) any acts or omissions of Contractor (or any of Contractor’s employees, agents, subcontractors, or by anyone else for whose acts any of them may be liable).

17.2 Indemnification Procedure. The State will notify Contractor in writing if indemnification is sought; however, failure to do so will not relieve Contractor, except to the extent that Contractor is materially prejudiced. Contractor must, to the satisfaction of the State, demonstrate its financial ability to carry out these obligations. The State is entitled to:

(a) regular updates on proceeding status;

(b) participate in the defense of the proceeding;

(c) employ its own counsel; and to

(d) retain control of the defense, at its own cost and expense, if the State deems necessary. Contractor will not, without the State’s prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. Any litigation activity on behalf of the State or any of its subdivisions, under this **Section 17**, must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

17.3 The State is constitutionally prohibited from indemnifying Contractor or any third parties.

18. Infringement Remedies.

18.1 The remedies set forth in this Section are in addition to, and not in lieu of, all other remedies that may be available to the State under this Contract or otherwise, including the State's right to be indemnified for such actions.

18.2 If any Software, Hardware, or any component thereof, other than State Materials, is found to be infringing or if any use of any Software or any component thereof is enjoined, threatened to be enjoined or otherwise the subject of an infringement claim, Contractor must, at Contractor's sole cost and expense:

(a) procure for the State the right to continue to use such Software, Hardware, or component thereof to the full extent contemplated by this Contract; or

(b) modify or replace the materials that infringe or are alleged to infringe ("**Allegedly Infringing Materials**") to make the Software, Hardware, and all of its components non-infringing while providing fully equivalent features and functionality.

18.3 If neither of the foregoing is possible notwithstanding Contractor's best efforts, then Contractor may direct the State to cease any use of any materials that have been enjoined or finally adjudicated as infringing, provided that Contractor will:

(a) refund to the State all amounts paid by the State in respect of such Allegedly Infringing Materials and any other aspects of the Software or Hardware provided under a Statement of Work for the Allegedly Infringing Materials that the State cannot reasonably use as intended under this Contract; and

(b) in any case, at its sole cost and expense, secure the right for the State to continue using the Allegedly Infringing Materials for a transition period of up to six (6) months to allow the State to replace the affected features of the Software or Hardware without disruption.

18.4 If Contractor directs the State to cease using any Software or Hardware under **Section 18.3**, the State may terminate this Contract for cause under **Section 16.1**. Unless the claim arose against the Software or Hardware independently of any of the actions specified below, Contractor will have no liability for any claim of infringement arising solely from:

(a) Contractor's compliance with any designs, specifications, or instructions of the State; or

(b) modification of the Software or Hardware by the State without the prior knowledge and approval of Contractor.

19. Disclaimer of Damages and Limitation of Liability.

19.1 The State's Disclaimer of Damages. THE STATE WILL NOT BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT FOR CONSEQUENTIAL, INCIDENTAL, INDIRECT, OR SPECIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOST PROFITS AND LOST BUSINESS OPPORTUNITIES.

19.2 The State's Limitation of Liability. IN NO EVENT WILL THE STATE'S AGGREGATE LIABILITY TO CONTRACTOR UNDER THIS CONTRACT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS CONTRACT, EXCEED THE MAXIMUM AMOUNT OF FEES PAYABLE UNDER THIS CONTRACT.

20. Disclosure of Litigation, or Other Proceeding. Contractor must notify the State within 14 calendar days of receiving notice of any litigation, investigation, arbitration, or other proceeding (collectively, "**Proceeding**") involving Contractor, a Permitted Subcontractor, or an officer or director of Contractor or Permitted Subcontractor, that arises during the term of the Contract, including:

- (a) a criminal Proceeding;
- (b) a parole or probation Proceeding;
- (c) a Proceeding under the Sarbanes-Oxley Act;
- (d) a civil Proceeding involving:
 - (i) a claim that might reasonably be expected to adversely affect Contractor's viability or financial stability; or
 - (ii) a governmental or public entity's claim or written allegation of fraud; or
- (e) a Proceeding involving any license that Contractor is required to possess in order to perform under this Contract.

21. State Data.

21.1 Ownership. The State's data ("**State Data**"), which will be treated by Contractor as Confidential Information, includes:

- (a) User Data; and
- (b) any other data collected, used, Processed, stored, or generated in connection with the Services, including but not limited to:
 - (i) personally identifiable information ("**PII**") collected, used, Processed, stored, or generated as the result of the Services, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements here listed; and
 - (ii) protected health information ("**PHI**") collected, used, Processed, stored, or generated as the result of the Services, which is defined under the Health Insurance Portability and Accountability Act ("**HIPAA**") and its related rules and regulations.

21.2 State Data is and will remain the sole and exclusive property of the State and all right, title, and interest in the same is reserved by the State.

21.3 Contractor Use of State Data.

(a) Contractor is provided a limited license to State Data for the sole and exclusive purpose of providing the Services, including a license to collect, process, store, generate, and display State Data only to the extent necessary in the provision of the Services. Contractor must:

- (i) keep and maintain State Data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss;
- (ii) use and disclose State Data solely and exclusively for the purpose of providing the Services, such use and disclosure being in accordance with this Contract, any applicable Statement of Work, and applicable law;
- (iii) keep and maintain State Data in the continental United States and
- (iv) not use, sell, rent, transfer, distribute, commercially exploit, or otherwise disclose or make available State Data for Contractor's own purposes or for the benefit of anyone other than the State without the State's prior written consent.

(b) Contractor must not copy, alter or remove any State Data from any State Systems without the State's express prior written authorization. The State, in its sole discretion, may revoke such authorization in writing at any time. Any State-authorized copying, alteration or removal of State Data must be solely in accordance with this Contract, in no case exceed the scope of the State's written authorization to Contractor, and must follow all instructions from the State, including but not limited any applicable State policies, standards, or procedures. Contractor must maintain complete and accurate records and audit logs relating to all such copying, alterations, and removals, and, upon the State's request, must provide all such records, audit logs, and other relevant materials to the State.

(c) Contractor's misuse of State Data may violate state or federal laws, including but not limited to MCL 752.795.

21.4 Discovery. Contractor will immediately notify the State upon receipt of any requests which in any way might reasonably require access to State Data or the State's use of the Software and Hosted Services, if applicable. Contractor will notify the State Program Managers or their designees by the fastest means available and also in writing. In no event will Contract provide such notification more than twenty-four (24) hours after Contractor receives the request. Contractor will not respond to subpoenas, service of process, FOIA requests, and other legal requests related to the State without first notifying the State and obtaining the State's prior approval of Contractor's proposed responses. Contractor agrees to provide its completed responses to the State with adequate time for State review, revision and approval.

21.5 Loss or Compromise of Data. In the event of any act, error or omission, negligence, misconduct, or breach on the part of Contractor that compromises or is suspected to compromise the security, confidentiality, integrity, or availability of State Data or the physical, technical, administrative, or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality, or integrity of State Data, Contractor must, as applicable:

- (a) notify the State as soon as practicable but no later than twenty-four (24) hours of becoming aware of such occurrence;
- (b) cooperate with the State in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by the State;
- (c) in the case of PII or PHI, at the State's sole election:

- (i) with approval and assistance from the State, notify the affected individuals who comprise the PII or PHI as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within five (5) calendar days of the occurrence; or
- (ii) reimburse the State for any costs in notifying the affected individuals;

(d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than twenty-four (24) months following the date of notification to such individuals;

(e) perform or take any other actions required to comply with applicable law as a result of the occurrence;

(f) pay for any costs associated with the occurrence, including but not limited to any costs incurred by the State in investigating and resolving the occurrence, including reasonable attorney's fees associated with such investigation and resolution;

(g) without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the occurrence;

(h) be responsible for recreating lost State Data in the manner and on the schedule set by the State without charge to the State; and

(i) provide to the State a detailed plan within ten (10) calendar days of the occurrence describing the measures Contractor will undertake to prevent a future occurrence. Notification to affected individuals, as described above, must comply with applicable law, be written in plain language, not be tangentially used for any solicitation purposes, and contain, at a minimum: name and contact information of Contractor's representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Contractor has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Contractor. The State will have the option to review and approve any notification sent to affected individuals prior to its delivery. Notification to any other party, including but not limited to public media outlets, must be reviewed and approved by the State in writing prior to its dissemination.

21.6 The parties agree that any damages relating to a breach of **Section 21** are to be considered direct damages and not consequential damages. **Section 21** survives termination or expiration of this Contract.

22. Non-Disclosure of Confidential Information. The parties acknowledge that each party may be exposed to or acquire communication or data of the other party that is confidential, privileged communication not intended to be disclosed to third parties. This **Section 22** survives termination or expiration of this Contract.

22.1 Meaning of Confidential Information. The term "**Confidential Information**" means all information and documentation of a party that:

(a) has been marked "confidential" or with words of similar meaning, at the time of disclosure by such party;

(b) if disclosed orally or not marked “confidential” or with words of similar meaning, was subsequently summarized in writing by the disclosing party and marked “confidential” or with words of similar meaning; or,

(c) should reasonably be recognized as confidential information of the disclosing party.

The term “Confidential Information” does not include any information or documentation that was or is:

(d) in the possession of the State and subject to disclosure under the Michigan Freedom of Information Act (FOIA);

(e) already in the possession of the receiving party without an obligation of confidentiality;

(f) developed independently by the receiving party, as demonstrated by the receiving party, without violating the disclosing party’s proprietary rights;

(g) obtained from a source other than the disclosing party without an obligation of confidentiality; or,

(h) publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure).

For purposes of this Contract, in all cases and for all matters, State Data is deemed to be Confidential Information.

22.2 Obligation of Confidentiality. The parties agree to hold all Confidential Information in strict confidence and not to copy, reproduce, sell, transfer, or otherwise dispose of, give or disclose such Confidential Information to third parties other than employees, agents, or subcontractors of a party who have a need to know in connection with this Contract or to use such Confidential Information for any purposes whatsoever other than the performance of this Contract. The parties agree to advise and require their respective employees, agents, and subcontractors of their obligations to keep all Confidential Information confidential. Disclosure to the Contractor’s subcontractor is permissible where:

(a) the subcontractor is a Permitted Subcontractor;

(b) the disclosure is necessary or otherwise naturally occurs in connection with work that is within the Permitted Subcontractor’s responsibilities; and

(c) Contractor obligates the Permitted Subcontractor in a written contract to maintain the State’s Confidential Information in confidence. At the State’s request, any of the Contractor’s and Permitted Subcontractor’s Representatives may be required to execute a separate agreement to be bound by the provisions of this **Section 22.2.**

22.3 Cooperation to Prevent Disclosure of Confidential Information. Each party must use its best efforts to assist the other party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the foregoing, each party must advise the other party immediately in the event either party learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Contract. Each party will cooperate with the other party in seeking injunctive or other equitable relief against any such person.

22.4 Remedies for Breach of Obligation of Confidentiality. Each party acknowledges that breach of its obligation of confidentiality may give rise to irreparable injury to the other party, which damage may be inadequately compensable in the form of monetary damages. Accordingly, a party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies which may be

available, to include, in the case of the State, at the sole election of the State, the immediate termination, without liability to the State, of this Contract or any Statement of Work corresponding to the breach or threatened breach.

22.5 Surrender of Confidential Information upon Termination. Upon termination or expiration of this Contract or a Statement of Work, in whole or in part, each party must, within five (5) Business Days from the date of termination, return to the other party any and all Confidential Information received from the other party, or created or received by a party on behalf of the other party, which are in such party's possession, custody, or control. Upon confirmation from the State, of receipt of all data, Contractor must permanently sanitize or destroy the State's Confidential Information, including State Data, from all media including backups using National Security Agency ("NSA") and/or National Institute of Standards and Technology ("NIST") (NIST Guide for Media Sanitization 800-88) data sanitation methods or as otherwise instructed by the State. If the State determines that the return of any Confidential Information is not feasible or necessary, Contractor must destroy the Confidential Information as specified above. The Contractor must certify the destruction of Confidential Information (including State Data) in writing within five (5) Business Days from the date of confirmation from the State.

23. Records Maintenance, Inspection, Examination, and Audit.

23.1 Right of Audit. Pursuant to MCL 18.1470, the State or its designee may audit Contractor to verify compliance with this Contract. Contractor must retain and provide to the State or its designee and the auditor general upon request, all financial and accounting records related to this Contract through the Term of this Contract and for four (4) years after the latter of termination, expiration, or final payment under this Contract or any extension ("**Financial Audit Period**"). If an audit, litigation, or other action involving the records is initiated before the end of the Financial Audit Period, Contractor must retain the records until all issues are resolved.

23.2 Right of Inspection. Within ten (10) calendar days of providing notice, the State and its authorized representatives or designees have the right to enter and inspect Contractor's premises or any other places where Services are being performed, and examine, copy, and audit all records related to this Contract. Contractor must cooperate and provide reasonable assistance. If financial errors are revealed, the amount in error must be reflected as a credit or debit on subsequent invoices until the amount is paid or refunded. Any remaining balance at the end of this Contract must be paid or refunded within forty-five (45) calendar days.

23.3 Application. This **Section 23** applies to Contractor, any Affiliate, and any Permitted Subcontractor that performs Services in connection with this Contract.

24. Support Services. Contractor will provide the State with the Support Services described in the Service Level Agreement attached as **Schedule D** to this Contract. Contractor acknowledges and agrees that it is responsible for providing the Support Services for all of the Software and Hardware provided under this Contract and to meet the requirements set forth in the SLA. Such Support Services will be provided:

(a) Free of charge during the Warranty Period.

(b) Thereafter, for so long as the State elects to receive Support Services for the Software and Hardware, in consideration of the State's payment of Fees for such services in accordance with the rates set forth in the Pricing Schedule.

25. Data Security Requirements. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor must comply with the requirements of the State's data security policies, standards and procedures as set forth in **Schedule E** to this Contract.

26. Training. Contractor will provide, at no additional charge, training on all uses of the Software and Hardware permitted hereunder in accordance with the times, locations and other terms set forth in a Statement of Work. Upon

the State's request, Contractor will timely provide training for additional Authorized Users or other additional training on all uses of the Software and Hardware for which the State requests such training, at such reasonable times and locations and pursuant to such rates and other terms as are set forth in the Pricing Schedule.

27. Maintenance Releases; New Versions

27.1 Maintenance Releases. Provided that the State is current on its Fees, during the Term, Contractor will provide the State, at no additional charge, with all Maintenance Releases, each of which will constitute Software and be subject to the terms and conditions of this Contract.

27.2 New Versions. Provided that the State is current on its Fees, during the Term, Contractor will provide the State, at no additional charge, with all New Versions, each of which will constitute Software and be subject to the terms and conditions of this Contract.

27.3 Installation. The State has no obligation to install or use any Maintenance Release or New Versions. If the State wishes to install any Maintenance Release or New Version, the State will have the right to have such Maintenance Release or New Version installed, in the State's discretion, by Contractor or other authorized party as set forth in a Statement of Work. Contractor will provide the State, at no additional charge, adequate Documentation for installation of the Maintenance Release or New Version, which has been developed and tested by Contractor and Accepted by the State. The State's decision not to install or implement a Maintenance Release or New Version of the Software will not affect its right to receive Support Services throughout the Term of this Contract.

28. Source Code Escrow

28.1 Escrow Contract. The parties may enter into a separate intellectual property escrow agreement. Such escrow agreement will govern all aspects of Source Code escrow and release. The cost of the escrow will be the sole responsibility of Contractor.

28.2 Deposit. Within thirty (30) business days of the Effective Date, Contractor will deposit with the escrow agent, pursuant to the procedures of the escrow agreement, the Source Code for the Software, as well as the Documentation and names and contact information for each author or other creator of the Software. Promptly after release of any update, upgrade, patch, bug fix, enhancement, new version, or other revision to the Software, Contractor will deposit updated Source Code, documentation, names, and contact information with the escrow agent.

28.3 Verification. At State's request and expense, the escrow agent may at any time verify the Deposit Material, including without limitation by compiling Source Code, comparing it to the Software, and reviewing the completeness and accuracy of any and all material. In the event that the Deposit Material does not conform to the requirements of **Section 28.2** above:

(a) Contractor will promptly deposit conforming Deposit Material; and

(b) Contractor will pay the escrow agent for subsequent verification of the new Deposit Material. Any breach of the provisions of this **Section 28.3** will constitute material breach of this Contract, and no further payments will be due from the State until such breach is cured, in addition to other remedies the State may have.

28.4 Deposit Material License. Contractor hereby grants the State a license to use, reproduce, and create derivative works from the Deposit Material, provided the State may not distribute or sublicense the Deposit Material or make any use of it whatsoever except for such internal use as is necessary to maintain and support the Software. Copies of the Deposit Material created or transferred pursuant to this Contract are licensed, not sold, and the State receives no title to or ownership of any copy or of the Deposit Material itself. The Deposit Material constitutes Confidential Information of Contractor pursuant to **Section 22** (Non-disclosure of Confidential Information) of this

Contract (provided no provision of **Section 22.4** calling for return of Confidential Information before termination of this Contract will apply to the Deposit Material).

29. Contractor Representations and Warranties.

29.1 Authority. Contractor represents and warrants to the State that:

- (a) It is duly organized, validly existing, and in good standing as a corporation or other entity as represented under this Contract under the laws and regulations of its jurisdiction of incorporation, organization, or chartering;
- (b) It has the full right, power, and authority to enter into this Contract, to grant the rights and licenses granted under this Contract, and to perform its contractual obligations;
- (c) The execution of this Contract by its Representative has been duly authorized by all necessary organizational action; and
- (d) When executed and delivered by Contractor, this Contract will constitute the legal, valid, and binding obligation of Contractor, enforceable against Contractor in accordance with its terms.
- (e) Contractor is neither currently engaged in nor will engage in the boycott of a person based in or doing business with a strategic partner as described in 22 USC 8601 to 8606.

29.2 Bid Response. Contractor represents and warrants to the State that:

- (a) The prices proposed by Contractor were arrived at independently, without consultation, communication, or agreement with any other Bidder for the purpose of restricting competition; the prices quoted were not knowingly disclosed by Contractor to any other Bidder to the Request for Proposal; and no attempt was made by Contractor to induce any other Person to submit or not submit a proposal for the purpose of restricting competition;
- (b) All written information furnished to the State by or for Contractor in connection with this Contract, including Contractor's Bid Response, is true, accurate, and complete, and contains no untrue statement of material fact or omits any material fact necessary to make the information not misleading;
- (c) Contractor is not in material default or breach of any other contract or agreement that it may have with the State or any of its departments, commissions, boards, or agencies. Contractor further represents and warrants that it has not been a party to any contract with the State or any of its departments that was terminated by the State within the previous five (5) years for the reason that Contractor failed to perform or otherwise breached an obligation of the contract; and
- (d) If any of the certifications, representations, or disclosures made in Contractor's Bid Response change after contract award, the Contractor is required to report those changes immediately to the Contract Administrator.

29.3 Software Representations and Warranties. Contractor further represents and warrants to the State that:

- (a) it is the legal and beneficial owner of the entire right, title and interest in and to its own Software, including all Intellectual Property Rights relating thereto;
- (b) it has, and throughout the license term, will retain the unconditional and irrevocable right, power and authority to grant and perform the license to its own Software hereunder;

(c) it has, and throughout the Term and any additional periods during which Contractor does or is required to perform the Services will have, the unconditional and irrevocable right, power and authority, including all permits and licenses required, to provide the Services and grant, provide, resell, and/or perform all rights and licenses provided or required to be provided by it under this Contract;

(d) the Software, and the State's use thereof, is and throughout the license term will be free and clear of all encumbrances, liens and security interests of any kind;

(e) neither its grant or provision of a license, nor its performance under this Contract does or to its knowledge will at any time:

- (i) conflict with or violate any applicable law;
- (ii) require the consent, approval or authorization of any governmental or regulatory authority or other third party; or
- (iii) require the provision of any payment or other consideration to any third party;

(f) when used by the State or any Authorized User in accordance with this Contract and the Documentation, the Software, the Hosted Services, if applicable, or Documentation as delivered or installed by Contractor does not or will not:

- (i) infringe, misappropriate, or otherwise violate any Intellectual Property Right or other right of any third party; or
- (ii) fail to comply with any applicable law;

(g) as provided by Contractor, the Software and Services do not and will not at any time during the Term contain any:

- (i) Harmful Code; or
- (ii) Third party or Open-Source Components that operate in such a way that it is developed or compiled with or linked to any third party or Open-Source Components, other than Approved Third Party Components specifically described in a Statement of Work.

(h) all Documentation is and will be complete and accurate in all material respects when provided to the State such that at no time during the license term will the Software have any material undocumented feature; and

(i) it will perform all Services in a timely, skillful, professional and workmanlike manner in accordance with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience and qualifications, and will devote adequate resources to meet its obligations under this Contract.

(j) when used in the Operating Environment (or any successor thereto) in accordance with the Documentation, all Software as provided by Contractor, will be fully operable, meet all applicable specifications, and function in all respects, in conformity with this Contract and the Documentation;

(k) Contractor acknowledges that the State cannot indemnify any third parties, including but not limited to any third-party software providers that provide software that will be incorporated in or otherwise used in conjunction with the Services, and that notwithstanding anything to the contrary contained in any third-party software license agreement or end user license agreement, the State will not indemnify any third party software provider for any reason whatsoever;

(l) no Maintenance Release or New Version, when properly installed in accordance with this Contract, will have a material adverse effect on the functionality or operability of the Software.

(m) all Configurations or Customizations made during the Term will be forward-compatible with future Maintenance Releases or New Versions and be fully supported without additional costs.

(n) During the Term of this Contract, any audit rights contained in any third-party software license agreement or end user license agreement for third-party software incorporated in or otherwise used in conjunction with the Software or with the Hosted Services, if applicable, will apply solely to Contractor or its Permitted Subcontractors. Regardless of anything to the contrary contained in any third-party software license agreement or end user license agreement, third-party software providers will have no audit rights whatsoever against State Systems or networks, unless agreed to by the State in writing.

29.4 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH IN THIS AGREEMENT, CONTRACTOR HEREBY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, WITH RESPECT TO THIS CONTRACT.

30. Offers of Employment. During the first twelve (12) months of the Contract, should Contractor hire an employee of the State who has substantially worked on any project covered by this Contract without prior written consent of the State, the Contractor will be billed for fifty percent (50%) of the employee's annual salary in effect at the time of separation.

31. Conflicts and Ethics. Contractor will uphold high ethical standards and is prohibited from: (a) holding or acquiring an interest that would conflict with this Contract; (b) doing anything that creates an appearance of impropriety with respect to the award or performance of the Contract; (c) attempting to influence or appearing to influence any State employee by the direct or indirect offer of anything of value; or (d) paying or agreeing to pay any person, other than employees and consultants working for Contractor, any consideration contingent upon the award of the Contract. Contractor must immediately notify the State of any violation or potential violation of these standards. This Section applies to Contractor, any parent, affiliate, or subsidiary organization of Contractor, and any Permitted Subcontractor that provides Services and Deliverables in connection with this Contract.

32. Compliance with Laws. Contractor, its subcontractors, including Permitted Subcontractors, and their respective Representatives must comply with all laws in connection with this Contract.

33. Nondiscrimination. Under the Elliott-Larsen Civil Rights Act, 1976 PA 453, MCL 37.2101, *et seq.*, the Persons with Disabilities Civil Rights Act, 1976 PA 220, MCL 37.1101, *et seq.*, and Executive Directive [2019-09](#), Contractor and its subcontractors agree not to discriminate against an employee or applicant for employment with respect to hire, tenure, terms, conditions, or privileges of employment, or a matter directly or indirectly related to employment, because of race, color, religion, national origin, age, sex, height, weight, marital status, partisan considerations, any mental or physical disability, or genetic information that is unrelated to the person's ability to perform the duties of a particular job or position. Breach of this covenant is a material breach of the Contract.

34. Unfair Labor Practice. Under MCL 423.324, the State may void any Contract with a Contractor or Permitted Subcontractor who appears on the Unfair Labor Practice register compiled under MCL 423.322.

35. Governing Law. This Contract is governed, construed, and enforced in accordance with Michigan law, excluding choice-of-law principles, and all claims relating to or arising out of this Contract are governed by Michigan law, excluding choice-of-law principles. Any dispute arising from this Contract must be resolved in the Michigan Court of Claims. Complaints against the State must be initiated in Ingham County, Michigan. Contractor waives any objections, such as lack of personal jurisdiction or *forum non conveniens*. Contractor must appoint an agent in Michigan to receive service of process.

36. Non-Exclusivity. Nothing contained in this Contract is intended nor is to be construed as creating any requirements contract with Contractor, nor does it provide Contractor with a right of first refusal for any future work. This Contract does not restrict the State or its agencies from acquiring similar, equal, or like Services from other sources.

37. Force Majeure

37.1 Force Majeure Events. Neither party will be liable or responsible to the other party, or be deemed to have defaulted under or breached the Contract, for any failure or delay in fulfilling or performing any term hereof, when and to the extent such failure or delay is caused by: acts of God, flood, fire or explosion, war, terrorism, invasion, riot or other civil unrest, embargoes or blockades in effect on or after the date of the Contract, national or regional emergency, or any passage of law or governmental order, rule, regulation or direction, or any action taken by a governmental or public authority, including imposing an embargo, export or import restriction, quota or other restriction or prohibition (each of the foregoing, a "**Force Majeure Event**"), in each case provided that: (a) such event is outside the reasonable control of the affected party; (b) the affected party gives prompt written notice to the other party, stating the period of time the occurrence is expected to continue; (c) the affected party uses diligent efforts to end the failure or delay and minimize the effects of such Force Majeure Event.

37.2 State Performance; Termination. In the event of a Force Majeure Event affecting Contractor's performance under the Contract, the State may suspend its performance hereunder until such time as Contractor resumes performance. The State may terminate the Contract by written notice to Contractor if a Force Majeure Event affecting Contractor's performance hereunder continues substantially uninterrupted for a period of five (5) Business Days or more. Unless the State terminates the Contract pursuant to the preceding sentence, any date specifically designated for Contractor's performance under the Contract will automatically be extended for a period up to the duration of the Force Majeure Event.

37.3 Exclusions; Non-suspended Obligations. Notwithstanding the foregoing or any other provisions of the Contract or this Schedule:

- (a) in no event will any of the following be considered a Force Majeure Event:
 - (i) shutdowns, disruptions or malfunctions of Hosted Services or any of Contractor's telecommunication or internet services other than as a result of general and widespread internet or telecommunications failures that are not limited to the Hosted Services; or
 - (ii) the delay or failure of any Contractor Personnel to perform any obligation of Contractor hereunder unless such delay or failure to perform is itself by reason of a Force Majeure Event.
- (b) no Force Majeure Event modifies or excuses Contractor's obligations under **Sections 21** (State Data), **22** (Non-Disclosure of Confidential Information), or **17** (Indemnification) of the Contract, Disaster Recovery and Backup requirements set forth in the Service Level Agreement, or any data retention or security requirements under the Contract.

38. Dispute Resolution. The parties will endeavor to resolve any Contract dispute in accordance with this provision. The dispute will be referred to the parties' respective Contract Administrators. Such referral must include a description of the issues and all supporting documentation. The parties must submit the dispute to a senior executive if unable to resolve the dispute within 15 business days. The parties will continue performing while a dispute is being resolved, unless the dispute precludes performance. A dispute involving payment does not preclude performance. Litigation to resolve the dispute will not be instituted until after the dispute has been elevated to the parties' senior executive and either concludes that resolution is unlikely or fails to respond within fifteen (15) business days. The parties are not prohibited from instituting formal proceedings: (a) to avoid the expiration of statute of limitations period; (b) to preserve a superior position with respect to creditors; or (c) where a party makes a determination that a temporary restraining order or other injunctive relief is the only adequate remedy. This Section does not limit the State's right to terminate the Contract.

39. Media Releases. News releases (including promotional literature and commercial advertisements) pertaining to this Contract or project to which it relates must not be made without the prior written approval of the State, and then only in accordance with the explicit written instructions of the State.

40. Severability. If any part of this Contract is held invalid or unenforceable, by any court of competent jurisdiction, that part will be deemed deleted from this Contract and the severed part will be replaced by agreed upon language that achieves the same or similar objectives. The remaining Contract will continue in full force and effect.

41. Waiver. Failure to enforce any provision of this Contract will not constitute a waiver.

42. Survival. The rights, obligations and conditions set forth in this **Section 42** and **Section 1** (Definitions), **Section 16.3** (Transition Responsibilities), **Section 17** (Indemnification), **Section 19** (Disclaimer of Damages and Limitations of Liability), **Section 21** (State Data), **Section 22** (Non-Disclosure of Confidential information), **Section 29** (Contractor Representations and Warranties), **Section 53** (Effect of Contractor Bankruptcy) and **Schedule C** Insurance, and any right, obligation or condition that, by its express terms or nature and context is intended to survive the termination or expiration of this Contract, survives any such termination or expiration.

43. Administrative Fee and Reporting Contractor must pay an administrative fee of 1% on all payments made to Contractor under the Contract including transactions with MiDEAL members, and other states (including governmental subdivisions and authorized entities).

Administrative fee payments must be made online by check or credit card at:
<https://www.thepayplace.com/mi/dtmb/adminfee>

Contractor must submit an itemized purchasing activity report, which includes at a minimum, the name of the purchasing entity and the total dollar volume in sales. Reports should be mailed to MiDeal@michigan.gov. The administrative fee and purchasing activity report are due within 30 calendar days from the last day of each calendar quarter.

44. Extended Purchasing Program. This contract is extended to MiDEAL members. MiDEAL members include local units of government, school districts, universities, community colleges, and nonprofit hospitals. A current list of MiDEAL members is available at www.michigan.gov/mideal.

Upon written agreement between the State and Contractor, this contract may also be extended to: (a) other states (including governmental subdivisions and authorized entities) and (b) State of Michigan employees.

If extended, Contractor must supply all Contract Activities at the established Contract prices and terms. The State reserves the right to impose an administrative fee and negotiate additional discounts based on any increased volume generated by such extensions.

Contractor must submit invoices to, and receive payment from, extended purchasing program members on a direct and individual basis.

45. Contract Modification. This Contract may not be amended except by signed agreement between the parties (a "Contract Change Notice"). Notwithstanding the foregoing, no subsequent Statement of Work or Contract Change Notice executed after the Effective Date will be construed to amend this Contract unless it specifically states its intent to do so and cites the section or sections amended.

46. HIPAA Compliance. The State and Contractor must comply with all obligations under HIPAA and its accompanying regulations, including but not limited to entering into a business associate agreement, if reasonably necessary to keep the State and Contractor in compliance with HIPAA.

47. Accessibility Requirements.

47.1 All Software provided by Contractor under this Contract, including associated content and documentation, must conform to WCAG 2.0 Level AA. Contractor must provide a description of conformance with WCAG 2.0 Level AA specifications by providing a completed PAT for each product provided under the Contract. At a minimum, Contractor must comply with the WCAG 2.0 Level AA conformance claims it made to the State, including the level of conformance provided in any PAT. Throughout the Term of the Contract, Contractor must:

- (a) maintain compliance with WCAG 2.0 Level AA and meet or exceed the level of conformance provided in its written materials, including the level of conformance provided in each PAT;
- (b) comply with plans and timelines approved by the State to achieve conformance in the event of any deficiencies;
- (c) ensure that no Maintenance Release, New Version, update or patch, when properly installed in accordance with this Contract, will have any adverse effect on the conformance of Contractor's Software to WCAG 2.0 Level AA;
- (d) promptly respond to and resolve any complaint the State receives regarding accessibility of Contractor's Software;
- (e) upon the State's written request, provide evidence of compliance with this Section by delivering to the State Contractor's most current PAT for each product provided under the Contract; and
- (f) participate in the State of Michigan Digital Standards Review described below.

47.2 State of Michigan Digital Standards Review. Contractor must assist the State, at no additional cost, with development, completion, and on-going maintenance of an accessibility plan, which requires Contractor, upon request from the State, to submit evidence to the State to validate Contractor's accessibility and compliance with WCAG 2.0 Level AA. Prior to the solution going-live and thereafter on an annual basis, or as otherwise required by the State, re-assessment of accessibility may be required. At no additional cost, Contractor must remediate all issues identified from any assessment of accessibility pursuant to plans and timelines that are approved in writing by the State.

47.3 Warranty. Contractor warrants that all WCAG 2.0 Level AA conformance claims made by Contractor pursuant to this Contract, including all information provided in any PAT Contractor provides to the State, are true and correct. If the State determines such conformance claims provided by the Contractor represent a higher level of conformance than what is actually provided to the State, Contractor will, at its sole cost and expense, promptly remediate its Software to align with Contractor's stated WCAG 2.0 Level AA conformance claims in accordance with plans and timelines that are approved in writing by the State. If Contractor is unable to resolve such issues in a manner acceptable to the State, in addition to all other remedies available to the State, the State may terminate this Contract for cause under **Section 16.1**.

47.4 Contractor must, without limiting Contractor's obligations of indemnification as further described in this Contract, indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State arising out of its failure to comply with the foregoing accessibility standards

47.5 Failure to comply with the requirements in this **Section 47** shall constitute a material breach of this Contract.

48. Further Assurances. Each party will, upon the reasonable request of the other party, execute such documents and perform such acts as may be necessary to give full effect to the terms of this Contract.

49. Relationship of the Parties. The relationship between the parties is that of independent contractors. Nothing contained in this Contract is to be construed as creating any agency, partnership, joint venture or other form of joint enterprise, employment or fiduciary relationship between the parties, and neither party has authority to contract for nor bind the other party in any manner whatsoever.

50. Headings. The headings in this Contract are for reference only and do not affect the interpretation of this Contract.

51. No Third-party Beneficiaries. This Contract is for the sole benefit of the parties and their respective successors and permitted assigns. Nothing herein, express or implied, is intended to or will confer on any other person or entity any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this Contract.

52. Equitable Relief. Each party to this Contract acknowledges and agrees that (a) a breach or threatened breach by such party of any of its obligations under this Contract may give rise to irreparable harm to the other party for which monetary damages would not be an adequate remedy and (b) in the event of a breach or a threatened breach by such party of any such obligations, the other party hereto is, in addition to any and all other rights and remedies that may be available to such party at law, at equity or otherwise in respect of such breach, entitled to equitable relief, including a temporary restraining order, an injunction, specific performance and any other relief that may be available from a court of competent jurisdiction, without any requirement to post a bond or other security, and without any requirement to prove actual damages or that monetary damages will not afford an adequate remedy. Each party to this Contract agrees that such party will not oppose or otherwise challenge the appropriateness of equitable relief or the entry by a court of competent jurisdiction of an order granting equitable relief, in either case, consistent with the terms of this Section.

53. Effect of Contractor Bankruptcy. All rights and licenses granted by Contractor under this Contract are and will be deemed to be rights and licenses to “intellectual property,” and all Software and Deliverables are and will be deemed to be “embodiments” of “intellectual property,” for purposes of, and as such terms are used in and interpreted under, Section 365(n) of the United States Bankruptcy Code (the “Code”). If Contractor or its estate becomes subject to any bankruptcy or similar proceeding, the State retains and has the right to fully exercise all rights, licenses, elections, and protections under this Contract, the Code and all other applicable bankruptcy, insolvency, and similar laws with respect to all Software and other Deliverables. Without limiting the generality of the foregoing, Contractor acknowledges and agrees that, if Contractor or its estate will become subject to any bankruptcy or similar proceeding:

(a) all rights and licenses granted to the State under this Contract will continue subject to the terms and conditions of this Contract, and will not be affected, even by Contractor's rejection of this Contract; and

(b) the State will be entitled to a complete duplicate of (or complete access to, as appropriate) all such intellectual property and embodiments of intellectual property comprising or relating to any Software or other Deliverables, and the same, if not already in the State's possession, will be promptly delivered to the State, unless Contractor elects to and does in fact continue to perform all of its obligations under this Contract.

54. Schedules. All Schedules that are referenced herein and attached hereto are hereby incorporated by reference. The following Schedules are attached hereto and incorporated herein:

Schedule A	Statement of Work
Schedule B	Pricing Schedule
Schedule C	Insurance Schedule
Schedule D	Service Level Agreement
Schedule E	Data Security Requirements
Schedule F	Transition Plan
Schedule G	Hardware

Schedule H
Schedule I

User Acceptance Testing
Software License Agreements

55. Counterparts. This Contract may be executed in counterparts, each of which will be deemed an original, but all of which together are deemed to be one and the same agreement and will become effective and binding upon the parties as of the Effective Date at such time as all the signatories hereto have signed a counterpart of this Contract. A signed copy of this Contract delivered by facsimile, e-mail or other means of electronic transmission (to which a signed copy is attached) is deemed to have the same legal effect as delivery of an original signed copy of this Contract.

56. Entire Agreement. These Terms and Conditions, including all Statements of Work and other Schedules and Exhibits (again collectively the "Contract") constitutes the sole and entire agreement of the parties to this Contract with respect to the subject matter contained herein, and supersedes all prior and contemporaneous understandings and agreements, representations and warranties, both written and oral, with respect to such subject matter. In the event of any inconsistency between the statements made in the Terms and Conditions, the Schedules, Exhibits, and a Statement of Work, the following order of precedence governs: (a) first, these Terms and Conditions and (b) second, Schedule E – Data Security Requirements and (c) third, each Statement of Work; and (d) fourth, the remaining Exhibits and Schedules to this Contract. NO TERMS ON CONTRACTOR'S (INCLUDING ITS SUBCONTRACTOR'S) INVOICES, WEBSITE, BROWSE-WRAP, SHRINK-WRAP, CLICK-WRAP, CLICK-THROUGH OR OTHER NON-NEGOTIATED TERMS AND CONDITIONS PROVIDED WITH ANY OF THE SERVICES, OR DOCUMENTATION HEREUNDER, EVEN IF ATTACHED TO STATE'S DELIVERY OR PURCHASE ORDER, WILL CONSTITUTE A PART OR AMENDMENT OF THIS CONTRACT OR IS BINDING ON THE STATE OR ANY AUTHORIZED USER FOR ANY PURPOSE. ALL SUCH OTHER TERMS AND CONDITIONS HAVE NO FORCE AND EFFECT AND ARE DEEMED REJECTED BY THE STATE AND THE AUTHORIZED USER, EVEN IF ACCESS TO OR USE OF SUCH SERVICE OR DOCUMENTATION REQUIRES AFFIRMATIVE ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

SCHEDULE A - STATEMENT OF WORK

1. DEFINITIONS

The following terms have the meanings set forth below. All initial capitalized terms that are not defined in this Schedule shall have the respective meanings given to them in Section 1 of the Contract Terms and Conditions.

Term	Definition
EOC-DC	Enterprise Operations Center – Data Center
LSHC	Lake Superior Hosting Center
LMHC	Lake Michigan Hosting Center
RFID	Radio Frequency Identification

2. BACKGROUND

The EOC-DC is responsible for the State hosting centers and certain supported telecom switch rooms. Contractor must provide software, hardware, licenses, maintenance, support, and integration for tools and must update and consolidate the physical and logical data center management and security tools around the State's existing Nlyte software management tool as specified in this Contract.

PURPOSE

The Contractor is providing a *State Hosted* Software Solution and applicable Hardware and Services. The Contractor must provide the following tools:

Nlyte DCIM suite – The Contractor must provide licenses and maintenance for the Nlyte modules. The State is currently invested in using the Nlyte Data Center Infrastructure Management (DCIM) modules, Nlyte Asset Optimizer (NAO) and Nlyte Energy Optimizer (NEO). NAO shall function as the primary asset management tool with this application providing a single point of contact as the asset “location of truth” for all other applications. Tools provided by Contractor under this Contract must be able to integrate with NEO and/or NAO for data exchange and provide information for dashboards, such as alarm notifications and camera views.

Visitor Management – The Contractor must provide a perpetual license for Technology Industries EntryPoint visitor management system. The visitor management system will contain profiles for individuals that have been vetted by the state and have authorization for access to controlled secure locations. Each visit provides specific data that assists staff in the review and authorization of the visit. When a visitor arrives at one of the controlled locations, they are checked in and are required to sign a signature pad, and when they leave, they are checked out. The EntryPoint application must provide functionality where each visitor provides a destination location/cabinet/device which is then validated within NAO. NAO compares the location of the asset, and the associated network and power connects in order to interface with the Rack Locking application for access control during the reservation time frame. The application will track tools with calendar managed inspection notifications, allow for the recording of assets entering and leaving a facility and visitor time sensitive documentation requirements. The application must also alarm upon over extension of visitor stay and provide a current list of active visitors with requested destinations for emergency response requirements. The visitor management system must meet specific audit requirements, based on NIST, CJIS and Pub 1075 controls.

Asset Control and physical audit – The Contractor must provide Asset Control and Physical Audit (RF Code) and Nlyte Asset Tagging for LSHC, LMHC and two Storage Rooms Readers for Depot, two Hannah Storage Rooms and Guard Station, RF Code will tie into Nlyte. The RF Code will provide real time and historical audit functionality and

alarming for unplanned asset motion and will provide an interface with the Nlyte applications through an SNMP connection for alarm notifications. The application must utilize live stored data from the NAO application as the "location of truth". This will allow the State of Michigan to have a separate auditable ability to track an asset location(s) over the asset's life cycle. RFID Tag functionality will provide a greater knowledge into the data center's environmental conditions, allow EOC-DC staff to plan and manage physical capacities, detect and manage changes, and provide greater physical security, all with the ability to analyze trends and reduce costs within EOC-DC managed spaces. The RFID Tagging and associated monitoring will allow staff the ability to electronically audit the current location of assets, "see" into the locations. The RFID tagging system will also provide notification if the asset(s) has/is being moved from one location to another from within the same room (cabinet to cabinet, room to room...) or if the RFID monitored asset leaves one building and enters a different building.

Environmental monitoring – The Contractor must provide Environmental Monitoring for LSHC consisting of RLE & Nlyte Wireless Temperature and Humidity Sensors (Every 3rd cabinet will have 3 temperature sensors on the front door, 3 on the rear door and 1 humidity sensor per aisle.) This application must electronically monitor the hosting center facility power and environmental delivery infrastructures. This application will be used by various groups to monitor and report incidents concerning the operation of the State of Michigan Hosting Center facilities power and environmental infrastructure. The application must notify by visual, audible, and electronic means the affected parties when an event occurs that affects the power delivery and environmental delivery systems. The application receives data from the modules via BACnet and Simple Network Management Protocol (SNMP) access over the State of Michigan's network. This function is in the process of being migrated to Nlyte Energy Optimizer (NEO) for the monitoring using Simple Network Management Protocol (SNMP) for data capture, therefore the requirement for this portion of the Contract is to provide the data collection modules.

Digital Video Management – The Contractor must provide a Milestone Video Surveillance System including a video management server and two network video recorders, eighty-four (84) surveillance cameras and Milestone Care Plus. The purpose of this system is to provide video capture, security, and access control at LSHC, LMHC and telecom switch rooms.

Rack Locking – The Contractor must provide Digitus Rack Locking for LSHC including Two-Factor Authentication and Integrating into Carrier's Lenel Software. The Rack Locking will integrate with the Nlyte NAO rack management system and visitor management system to be able to identify the proper rack that needs to be unlocked for a technician's visit. The Rack Locking application must interface with the Visitor Management, NAO and Asset Control and physical audit applications to provide a consistent security presence for allowing planned operations to proceed and alarming for unplanned changes or access attempts.

Required Tool Summary	Vendor Tool Name Summary
Nlyte DCIM suite	Nlyte
Visitor Management	Technology Industries (EntryPoint)
Asset Control and physical audit	RFCode
Environmental monitoring	RLE Technologies
Digital Video Management	Milestone
Rack Locking	Digitus

3. IT ENVIRONMENT RESPONSIBILITIES

Included in **SCHEDULE E – Data Security Agreement**; the Contractor will be required to meet all applicable State PSP's, public and non-public.

For a State Hosted Software Solution:

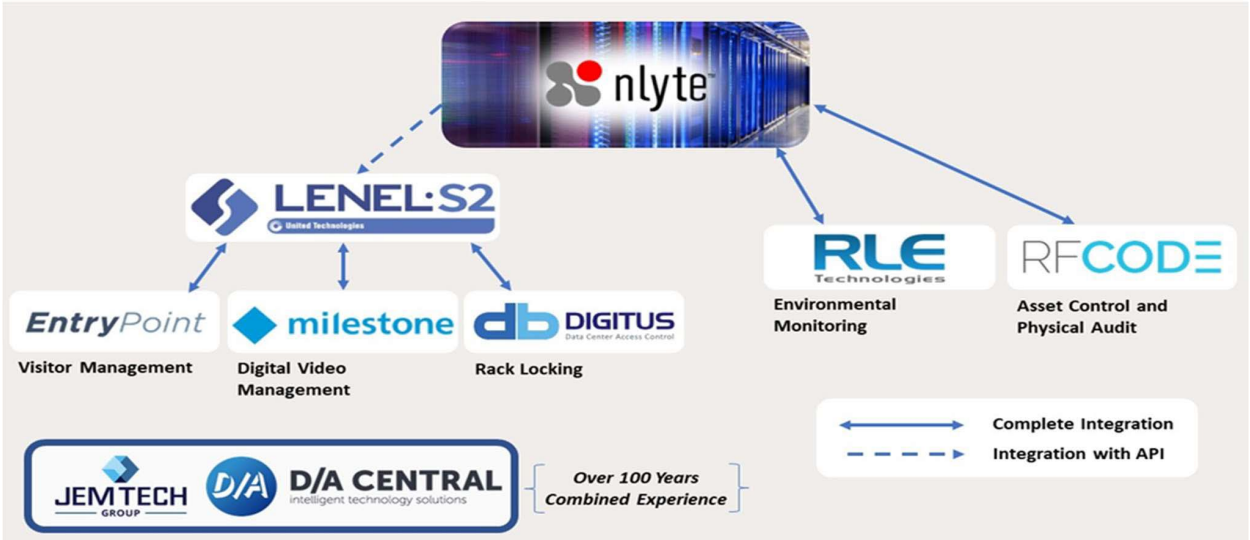
Definitions:

Application – Software programs which provide functionality for end user and Contractor services.

Development - Process of creating, testing and maintaining software components.

Component Matrix	Disclose subcontractor name(s), if applicable.
Application/Development	Nlyte Lenel EntryPoint Milestone Digitus RLE RF Code D/A Central

State of Michigan’s Ecosystem for EOC-DC Tools



Contractor will perform integration of RfCode and RLE into Nlyte. Digitus, Milestone and EntryPoint all have software integrations into Lenel. There will be an API integration from Lenel into Nlyte. Contractor will assume responsibility for all software and hardware purchased under this Contract.

4. ADA COMPLIANCE

The State is required to comply with the Americans with Disabilities Act of 1990 (ADA) and has adopted standards and procedures regarding accessibility requirements for websites and software applications. All websites, applications, software, and associated content and documentation provided by the Contractor as part of the Solution must comply with Level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.0.

5. USER TYPE AND CAPACITY

Type of User	Access Type	Number of Users	Number of Concurrent Users
Public Citizen	None	0	0

State Personnel	R,W,A	55	10
-----------------	-------	----	----

Contractor Solution must meet the expected number of concurrent Users.

6. ACCESS CONTROL AND AUTHENTICATION

The Contractor’s solution must integrate with the State’s IT Identity and Access Management (IAM) environment as described in the State of Michigan Digital Strategy 1340.00.020.08 Enterprise Identity and Access Management Services Standard (michigan.gov) , which consist of:

- 6.1 MILogin/Michigan Identity, Credential, and Access Management (MICAM). An enterprise single sign-on and identity management solution based on IBM’s Identity and Access Management products including, IBM Security Identity Manager (ISIM), IBM Security Access Manager for Web (ISAM), IBM Tivoli Federated Identity Manager (TFIM), IBM Security Access Manager for Mobile (ISAMM), and IBM DataPower, which enables the State to establish, manage, and authenticate user identities for the State’s Information Technology (IT) systems.
- 6.2 MILogin Identity Federation. Allows federated single sign-on (SSO) for business partners, as well as citizen-based applications.
- 6.3 MILogin Multi Factor Authentication (MFA, based on system data classification requirements). Required for those applications where data classification is Confidential and Restricted as defined by the 1340.00 Michigan Information Technology Information Security Policy (i.e. the proposed solution must comply with PHI, PCI, CJIS, IRS, and other standards).
- 6.4 MILogin Identity Proofing Services (based on system data classification requirements). A system that verifies individual’s identities before the State allows access to its IT system. This service is based on “life history” or transaction information aggregated from public and proprietary data sources. A leading credit bureau provides this service.

To integrate with the SOM MILogin solution, the Contractor’s solution must support SAML, or OAuth or OpenID interfaces for the SSO purposes.

7. DATA RETENTION AND REMOVAL

The State will need to retain all data for the entire length of the Contract unless otherwise directed by the State.

The State will need the ability to delete data, even data that may be stored off-line or in backups.

The State will need to retrieve data, even data that may be stored off-line or in backups.

8. END USER AND IT OPERATING ENVIRONMENT

The SOM IT environment includes X86 VMware, IBM Power VM, MS Azure/Hyper-V and Oracle VM, with supporting platforms, enterprise storage, monitoring, and management running in house and in cloud hosting provides.

Contractor must accommodate the latest browser versions (including mobile browsers) as well as some pre-existing browsers. To ensure that users with older browsers are still able to access online services, applications must, at a minimum, display and function correctly in standards-compliant browsers and the state standard browser without the use of special plugins or extensions. The rules used to base the minimum browser requirements include:

- Over 2% of desktop and mobile & tablet site traffic, measured using Michigan.gov sessions statistics and
- The current browser identified and approved as the State of Michigan standard

This information can be found at <https://www.michigan.gov/browserstats>. Please use the most recent calendar quarter to determine browser statistics. For those desktop and mobile & tablet browsers with over 2% of site traffic, except Internet Explorer which requires support for at minimum version 11, the current browser version as well as the previous two major versions must be supported.

Contractor must support the current and future State standard environment at no additional cost to the State.

9. SOFTWARE

Software requirements are identified in **Schedule A – Table 1 Business Specification Worksheet**.

Contractor must provide a list of any third party components, and open source component included with or used in connection with the deliverables defined within this Contract. This information must be provided to the State on a quarterly basis and/or if a new third party or open source component is used in the performance of this Contract.

Look and Feel Standards

All software items provided by the Contractor must adhere to the State of Michigan Application/Site standards which can be found at <https://www.michigan.gov/standards>.

Mobile Responsiveness

If the software will be used on a mobile device as define in Schedule A – Table 1, Business Specification Worksheet, the Software must utilize responsive design practices to ensure the application is accessible via a mobile device.

SOM IT Environment Access

Contractor must access State environments using one or more of the following methods:

- State provided VDI (Virtual Desktop Infrastructure) where compliant.
- State provided and managed workstation device.
- Contractor owned and managed workstation maintained to all State policies and standards.
- Contractor required interface with State systems which must be maintained in compliance with State policies and standards as set forth in **Schedule E – Data Security Requirements**.
- Contractor must access State environments from locations within the United States and jurisdiction territories.

Security management platform software:

- Access Control and integration platform – Lenel OnGuard Ver 8.1
- Visitor Management – EntryPoint Ver 5.9
- Video Management System – Milestone XProtect Corporate 2022 R2

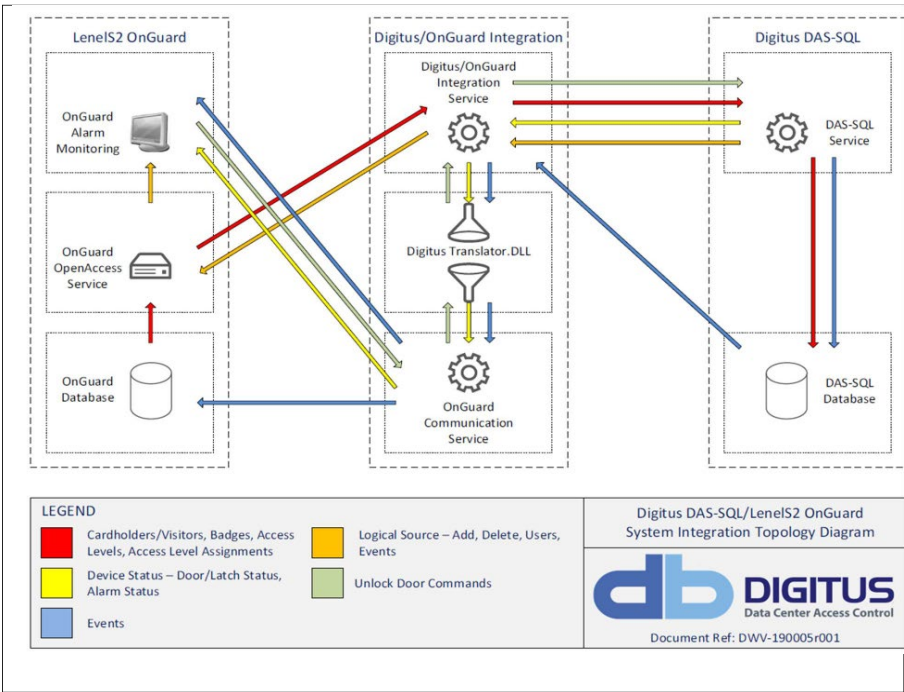
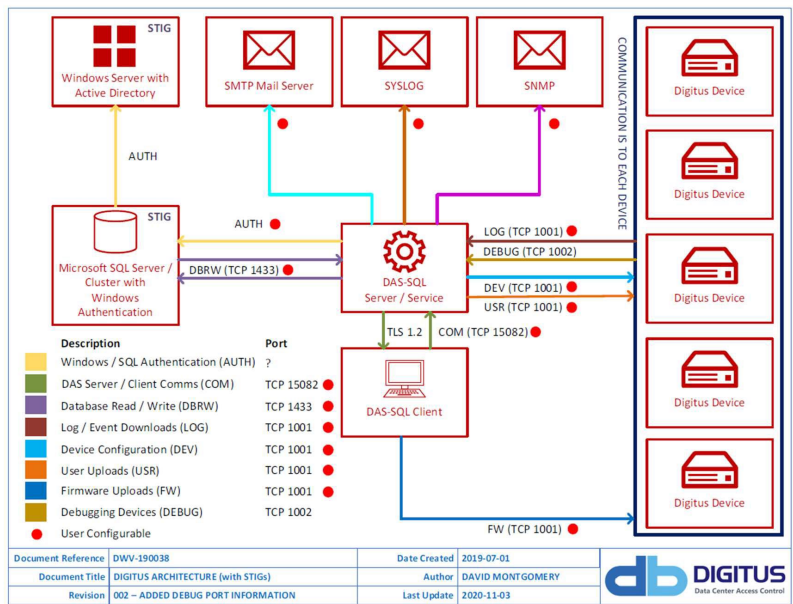
Architecture and functional design: The Lenel OnGuard security management system will provide the foundation for integration between the proposed security functions (Rack locking, visitor management, video management) of the system. It will store and manage access rights to connected Digitus locking hardware and store access control logs for both SOM credential holders and visitors. It will contain the profiles for individuals that have been vetted by the state and have authorization for access to controlled secure locations.

The Digitus Server Rack Access Control System, Milestone Video Management System (VMS), and EntryPoint Visitor Management (VM) will all integrate into the Lenel OnGuard Access Control System (ACS) through their API. These integrations have all been approved and certified by Lenel through their partner program. All pertinent information required by the Nlyte Data Center Infrastructure Management (DCIM) will be pushed into Nlyte via SNMP, through the Nlyte API and/or SQL Database Access with read/write capabilities.

The visitor management integration updates the OnGuard database based on input from staff when a visitor arrives. Each visit provides specific data that assists staff in the review and authorization of the visit. The visitor management system will track tools and equipment accompanying a visitor. The visitor management integration provides the UI for staff to check in visitors, add new visitors, check out visitors, be notified of visitors who require special handling, send notification that a visitor has overstayed, and collect the required data to comply with specific audit requirements,

based on NIST, CJIS and Pub 1075 controls.

The Digitus DAS-SQL Access Control Solution is a full-featured Access Control System that uses PINs, fingerprint identification and high and low frequency RFID cards to control locking doors. The Digitus DAS-SQL Management Platform is a client-server application that uses Microsoft SQL Server for its databases. A single DAS-SQL Server supports connections from multiple administrative clients and can manage multiple sites. The Digitus DAS-SQL Server uploads device configuration information, Timebands and Users to the Devices (Controller hardware) and monitors the status of all Devices, retrieving state and event logs (access attempts, alarms, and other events). DAS-SQL Clients (workstations) are used to configure, manage and monitor the system.



10. INTEGRATION

Contractor must integrate their solution to the following technologies:

Current Technology	All applications must be able to integrate with Nlyte Asset Optimizer for “location of truth” determination.
Volume of Data	The volume of data shall be determined by the requirements of the application querying Nlyte Asset Optimizer (NAO) and/or Nlyte Energy Optimizer (NEO) for either data pushes to or pulled data from the NAO/NEO SQL Databases. The time frequency will be determined upon an event based criteria and the requesting applications pre-determined requirements per State of Michigan business requirements.
Format of the input & export files	The format shall be compatible with Nlyte or a pre-determined SQL access event.

11. TRAINING SERVICES

The Contractor must provide administration and end-user training for implementation, go-live support, and transition to customer self-sufficiency.

12. TRANSITION RESPONSIBILITIES

Upon termination or expiration of the agreement, Contractor must, for a period of time specified by the State (not to exceed 90 calendar days), provide all reasonable transition assistance requested by the State, to allow for the expired or terminated portion of the agreement to continue without interruption or adverse effect, and to facilitate the orderly transfer of the services to the State or its designees. Such transition assistance may include but is not limited to: (a) continuing to perform the services at the established rates; (b) taking all reasonable and necessary measures to transition performance of the work, including all applicable services to the State or the State’s designee; (c) taking all necessary and appropriate steps, or such other action as the State may direct, to preserve, maintain, protect, or return (in a format specified by the State) to the State all data stored in the solution; and (d) preparing an accurate accounting from which the State and Contractor may reconcile all outstanding accounts.

13. DOCUMENTATION

Contractor must provide all user manuals, operating manuals, technical manuals and any other instructions, specifications, documents or materials, in any form or media, that describe the functionality, installation, testing, operation, use, maintenance, support, technical or other components, features or requirements of the Software.

Contractor must develop and submit for State approval complete, accurate, and timely Solution documentation to support all users, and will update any discrepancies, or errors through the life of the contract.

The Contractor’s user documentation must provide detailed information about all software features and functionality, enabling the State to resolve common questions and issues prior to initiating formal support requests.

14. RESERVED

15. CONTRACTOR PERSONNEL

Contractor Contract Administrator. Contractor resource who is responsible to(a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

JEM Tech Group
Jami Moore 23537 Lakepointe Dr., Clinton Twp., MI 48036 (586) 783-3400 j.moore@jemtechgroup.com

16. CONTRACTOR KEY PERSONNEL

Contractor Project Manager. Contractor resource who is responsible to serve as the primary contact with regard to services who will have the authority to act on behalf of the Contractor in matters pertaining to the implementation services, matters pertaining to the receipt and processing of Support Requests and the Support Services.

JEM Tech Group
Nick Notoriano 23537 Lakepointe Dr., Clinton Twp., MI 48036 (586) 783-3400 n.notoriano@jemtechgroup.com Alternative Contact: Shelley Deane 23537 Lakepointe Dr., Clinton Twp., MI 48036 (586) 783-3400 s.deane@jemtechgroup.com

Contractor Security Officer. Contractor resource who is responsible to respond to State inquiries regarding the security of the Contractor’s Solution. This person must have sufficient knowledge of the security of the Contractor Solution and the authority to act on behalf of Contractor in matters pertaining thereto.

JEM Tech Group
Nick Notoriano 23537 Lakepointe Dr., Clinton Twp., MI 48036 (586) 783-3400 n.notoriano@jemtechgroup.com Alternative Contact: Shelley Deane 23537 Lakepointe Dr., Clinton Twp., MI 48036 (586) 783-3400 s.deane@jemtechgroup.com

17. CONTRACTOR PERSONNEL REQUIREMENTS

Background Checks. Contractor must present certifications evidencing satisfactory Michigan State Police Background checks, ICHAT, and drug tests for all staff identified for assignment to this project.

In addition, proposed Contractor personnel will be required to complete and submit an RI-8 Fingerprint Card for the National Crime Information Center (NCIC) Finger Prints, if required by project.

Contractor will pay for all costs associated with ensuring their staff meets all requirements.

Offshore Resources.

Contractor will not be using any offshore resources

Disclosure of Subcontractors. If the Contractor intends to utilize subcontractors, the Contractor must disclose the following:

- The legal business name; address; telephone number; a description of subcontractor’s organization and the services it will provide; and information concerning subcontractor’s ability to provide the Contract Activities.
- The relationship of the subcontractor to the Contractor.
- Whether the Contractor has a previous working experience with the subcontractor. If yes, provide details of that previous relationship.
- A complete description of the Contract Activities that will be performed or provided by the subcontractor.

Contractor will use the following Permitted Subcontractors for the purposes stated below:

The legal business name, address, telephone number of the Permitted Subcontractor.	D/A Central 13155 Cloverdale Street Oak Park, MI 48237 248-399-0600
A complete description of the Contract Activities that will be performed or provided by the Permitted Subcontractor.	JEM will be subcontracting with D/A for the following tools: Lenel, Milestone (Digital Video Management), and Technology Industries/EntryPoint (Visitor Management).
The legal business name, address, telephone number of the Permitted Subcontractor.	Nlyte 1150 Roberts Blvd. Kennesaw, GA 30144 732-395-6920
A complete description of the Contract Activities that will be performed or provided by the Permitted Subcontractor.	JEM will be subcontracting with Nlyte to provide licenses and maintenance for the Nlyte modules (Data Center Infrastructure Management (DCIM) modules and Nlyte Asset Optimizer (NAO) and Nlyte Energy Optimizer (NEO)
The legal business name, address, telephone number of the Permitted Subcontractor.	RF Code 9229 Waterford Centre Suite 500 Austin, TX 78758 512-439-2200
A complete description of the Contract Activities that will be performed or provided by the Permitted Subcontractor.	JEM will be subcontracting with RF Code to provide Asset Control and Physical Audit.
The legal business name, address, telephone number of the Permitted Subcontractor.	RLE Technologies 104 Racquette Drive Fort Collins, CO 80524 970-484-6510

A complete description of the Contract Activities that will be performed or provided by the Permitted Subcontractor.	JEM will be subcontracting with RLE Technologies for Environmental Monitoring hardware
The legal business name, address, telephone number of the Permitted Subcontractor.	Digitus 25 Bull St Ste 700 Savannah, GA 31401 912-231-8175
A complete description of the Contract Activities that will be performed or provided by the subcontractor.	JEM will be subcontracting with Digitus to provide Rack Locking
The legal business name, address, telephone number of the Permitted Subcontractor.	Milestone 5300 Meadows Rd, Suite 400, Lake Oswego, Oregon 97035 503-350-1100
A complete description of the Contract Activities that will be performed or provided by the Permitted Subcontractor.	JEM will be subcontracting with D/A Central who will be subcontracting with Milestone to provide a Video Surveillance System.
The legal business name, address, telephone number of the Permitted Subcontractor.	Technology Industries (EntryPoint) 814 King Street 3rd Floor Alexandria, VA 22314 571-354-8884
A complete description of the Contract Activities that will be performed or provided by the Permitted Subcontractor.	JEM will be subcontracting with D/A Central who will be subcontracting with Technology Industries (EntryPoint) to provide a Visitor Management solution
The legal business name, address, telephone number of the Permitted Subcontractor.	Lenel 1212 Pittsford-Victor Road Pittsford, New York 14534 866-788-5095
A complete description of the Contract Activities that will be performed or provided by the Permitted Subcontractor.	JEM will be subcontracting with D/A Central who will be subcontracting with Lenel which will provide the integration between the Rack locking, visitor management, video management.

18. STATE RESOURCES/RESPONSIBILITIES

The State will provide the following resources as part of the implementation and ongoing support of the Solution.

State Contract Administrator. The State Contract Administrator is the individual appointed by the State to (a) administer the terms of this Contract, and (b) approve and execute any Change Notices under this Contract.

State Contract Administrator
Shannon Romein 517-898-8102 RomeinS@michigan.gov

Program Managers. The Program Managers (or designee) will jointly approve all Deliverables and day to day activities.

Program Manager
Jennifer Poirier 517-242-2417 poirierj@michigan.gov

Program Manager Designee
Melissa Hoodhood 517-930-0687 hoodhoodm@michigan.gov

19. MEETINGS

At start of the engagement, the Contractor Project Manager must facilitate a project kick off meeting with the support from the State's Project Manager and the identified State resources to review the approach to accomplishing the project, schedule tasks and identify related timing, and identify any risks or issues related to the planned approach. From project kick-off until final acceptance and go-live, Contractor Project Manager must facilitate weekly meetings (or more if determined necessary by the parties) to provide updates on implementation progress. Following go-live, Contractor must facilitate monthly meetings (or more or less if determined necessary by the parties) to ensure ongoing support success.

The Contractor must attend the following meetings, at a location and time as identified by the state, at no additional cost to the State:

- Kick-off meeting, 10 days after contract has been signed
- Weekly or bi-weekly implementation progress meetings

20. PROJECT CONTROL & REPORTS

Once the Project Kick-Off meeting has occurred, the Contractor Project Manager will monitor project implementation progress and report on a weekly basis to the State's Project Manager the following:

- Progress to complete milestones, comparing forecasted completion dates to planned and actual completion dates
- Accomplishments during the reporting period, what was worked on and what was completed during the current reporting period
- Indicate the number of hours expended during the past week, and the cumulative total to date for the project. Also, state whether the remaining hours are sufficient to complete the project
- Tasks planned for the next reporting period
- Identify any existing issues which are impacting the project and the steps being taken to address those issues
- Identify any new risks and describe progress in mitigating high impact/high probability risks previously identified
- Indicate the amount of funds expended during the current reporting period, and the cumulative total to date for the project.

21. PROJECT MANAGEMENT

The Contractor Project Manager will be responsible for maintaining a project schedule (or approved alternative) identifying tasks, durations, forecasted dates and resources – both Contractor and State - required to meet the timeframes as agreed to by both parties.

Changes to scope, schedule or cost must be addressed through a formal change request process with the State and the Contractor to ensure understanding, agreement and approval of authorized parties to the change and clearly identify the impact to the overall project.

SUITE Documentation

In managing its obligation to meet the above milestones and deliverables, the Contractor is required to utilize the applicable [State Unified Information Technology Environment \(SUITE\)](#) methodologies, or an equivalent methodology proposed by the Contractor.

SUITE's primary goal is the delivery of on-time, on-budget, quality systems that meet customer expectations. SUITE is based on industry best practices, including those identified in the Project Management Institute's PMBoK and the Capability Maturity Model Integration for Development. It was designed and implemented to standardize methodologies, processes, procedures, training, and tools for project management and systems development lifecycle management. It offers guidance for efficient, effective improvement across multiple process disciplines in the organization, improvements to best practices incorporated from earlier models, and a common, integrated vision of improvement for all project and system related elements.

While applying the SUITE framework through its methodologies is required, SUITE was not designed to add layers of complexity to project execution. There should be no additional costs from the Contractor, since it is expected that they are already following industry best practices which are at least similar to those that form SUITE's foundation.

SUITE's companion templates are used to document project progress or deliverables. In some cases, Contractors may have in place their own set of templates for similar use. Because SUITE can be tailored to fit specific projects, project teams and State project managers may decide to use the Contractor's provided templates, as long as they demonstrate fulfillment of the SUITE methodologies.

Milestones/Deliverables for Implementation

The State's milestone schedule and associated deliverables are in Schedule B. Acceptance is defined in Schedule H: USER ACCEPTANCE TESTING

22. ENVIRONMENTAL AND ENERGY EFFICIENCY PRODUCT STANDARDS

Environmental and Energy Efficiency Product Standards

There are no environmental and energy efficient standards for this purchase

Hazardous Chemical Identification

There are no hazardous chemicals for this purchase.

Mercury Content

There are no mercury containing products for this purchase.

Brominated Flame Retardants

There are no brominated flame retardants (BFRs) or Perfluoroalkyl and Polyfluoroalkyl Substances (PFAS) for this purchase.

23. Hardware

Please see Schedule G – Hardware for more details on hardware requirements.

Visitor Management and Digital Video Management (DVM)		
Part #	Qty	Description
DVM	1	The Video Surveillance System including a video management server and 2 network video recorders, and eighty-four (84) surveillance cameras. Recording will be aggregated at the Lake Superior Hosting Center with redundancy (backup server) installed at Lake Michigan Hosting Center.
VM	1	Visitor Management System including two (2) kiosk workstations to be installed at LSHC and LMHC

Asset Control and Physical Audit (RFCode)& Nlyte Asset Tagging		
Part #	Qty	Description
RF CODE_ASSET_TAG	1	RF Code To Include: (25) M250 433 MHz Reader Kit (216) Rack Locator Kit for 40U Racks (70-in) (216) A740 Rack Locator Controller Unit (216) A740 Power Supply (432) Rack Locator LED Strip with blue indicators, 70" for 40U racks (9) Rack Locator Kit for 44U Racks (77-in) (9) A740 Rack Locator Controller Unit (9) A740 Power Supply (18) Rack Locator LED Strip with blue indicators, 77" for 44U racks (18) Rack Locator Kit for 47U Racks (82.25-in) (18) A740 Rack Locator Controller Unit (18) A740 Power Supply (36) Rack Locator LED Strip w blue indicators, 82.25" for 47U racks (243) A740 Extension Cable (60 inch) M/F 3.5mm (243) A740 Signal Splitter (2287) IR-Enabled IT Asset Sensor Only (2400) Flag Tab (4 inch) (200) Thumb Screw Tab (200) Thin Loop Tab (Feed-Thru) (10) Tab Install Keys for M174 IT Asset Loc Sensor (5 Keys) (216) Rack Locator LED Strip with blue indicators,70" for 40U racks

Environmental Monitoring for LSHC (RLE & Nlyte)

Part #	Qty	Description
WiNG-MGR	3	WiNG Manager - 900MHz receiver; includes rack mount bracket, PSWA-DC-24 power supply and type A blade
WiNG-RXT	1	WiNG Range Extender, 900 MHz signals, includes PSWA-DC-5 power supply and type A blade
WiNG-TH	102	WiNG Temperature/Humidity sensor; 900 MHz wireless transmitter
WiNG-LD-LC	17	WiNG Leak Detector; 900 MHz wireless transmitter, includes LC-KIT, requires SC, SC-R, SC-ZH or SD-Z
SC-50	17	SeaHawk Sensing Cable; conductive fluids, 50ft (15.24m), pre-installed male/female connectors

JC-10	17	J-Clips; qty 10 (for use with SC, SC-R, SC-ZH and NSC)
-------	----	--

Rack Locking for LSHC Two-Factor Authentication (Pin Code & Card Swipe)

Part #	Qty	Description
dbSENTRY-KH KH(S)	240	Cabinet Sentry w/2 Dual Lock Swing Handles (S), 2 Door Contacts, 1 CAT5e Cable 14', Cable Tie Downs, db Sentry Cabinet, and RFID Swing Handle Cabinets are APC & CPI
dbSENTRY-KH(S)	2	Cabinet Sentry w/ 1 CodeLock-HF Swing Handle (S), 1 Door Contact, 1 CAT5e Cable 14', Cable Tie Downs, db Sentry Cabinet, and RFID Swing Handle APC wall mounted Cabinets
dbSentry-KRKR -R4R4	49	Cabinet Sentry w/2 Dual Readers & 2 R4 Latch Kits, 2 Door Contacts, 1 CAT 5e Cable Tie Downs for 21 Floor PDUs, 12 EMC and 7 Teradata Cabinets
db Power	291	Auxiliary Power Supply for db Sentry 110V or 208V
dbDC10	240	Surface Mount Door Contacts no resistors and no wires, (only needed if there are split rear doors)
dbDC1W	122	Door Contacts (10K) with wires Side panel contacts. Assumes 1 panel per side
dbLOGI-500	1	DAS server/client package & LENEL OnGuard Integration Software for connection up to 500 units
OK5427 V2	1	Omniquey 5427 V2 Multi-class Card Reader/Writer
dbDASSQL-CR W	9	DAS Server/Client package including a card reader/writer
dbINF-SR	1	db Infinity Maintenance Service - from Shipment of Handles to LSHC

24. ADDITIONAL INFORMATION

The State reserves the right to purchase any additional services or products from the Contractor during the duration of the Contract.

SCHEDULE A – TABLE 1 - Business Specification Worksheet

This Business Specifications Worksheet contains the requirements for the tools that the Contractor must provide under this Contract.

Column A: System

Column B: Business Specification Number.

Column C: Detailed Business Requirement Description

System	Business Req. No.	Detailed Business Requirement Description
Digital Video Management	0.0 Disaster Recovery of capture device (Camera)	
Digital Video Management		
Digital Video Management	0.0.1 Loss of Power to Cameras	
Digital Video Management	0.0.1.1	Alarms provided to EOC-DC Management for the following for each occurrence at the time of occurrence:
Digital Video Management	0.0.1.2	Hot hand off of occurrence notification
Digital Video Management	0.0.1.3	Communication methods are phone with Remedy ticket notification to follow
Digital Video Management	0.0.1.4	Time/Date of event occurrence
Digital Video Management	0.0.1.5	Remedy Incident / Emergency Request for Change (RFC) number shall be provided
Digital Video Management	0.1.6	List of Device(s) affected
Digital Video Management	0.1.7	Estimated Time of Return to Operation
Digital Video Management	0.1.8	Time/Date of validated return to operation
Digital Video Management	0.1.9	Post mortem RCA with results documented as following
Digital Video Management	0.1.9.1	Providing all steps and communication activity for issue remediation
Digital Video Management	0.1.10	Current and future activity to eliminate the re-occurrence of event
Digital Video Management	0.1.11	Sign off from EOC-DC Management of event conclusion and resolution

Digital Video Management	0.2	In the event of a loss of communication with the management server(s) but the capture device remains powered local to the capture device storage shall be utilized with uploading capability once communication is reestablished with Management Server(s)
Digital Video Management	0.2.1	See 0.0.1.0 – 0.0.1.11
Digital Video Management	1 Security Posture	
Digital Video Management	1.1 Access controls	
Digital Video Management	1.1.1	All access is to be managed
Digital Video Management	1.1.1.1	Access to client consoles and/or pre-determined designed view is to be managed via SLDAP AD Group(s)
Digital Video Management		
Digital Video Management	1.1.1.2	All access to views within EOC-DC managed locations are to be pre-determined by the following:
Digital Video Management		
Digital Video Management	1.1.1.2.1	<ul style="list-style-type: none"> • Job description for view access • Criticality of camera view • All Access is approved by EOC-DC Management
Digital Video Management		
Digital Video Management		
Digital Video Management		
Digital Video Management		
Digital Video Management	2	
Digital Video Management	Clip Retention	
Digital Video Management	2.1	
Digital Video Management	All video capture clip retention is to be defined on a point by point basis as determined by EOC-DC Management for the following	
Digital Video Management	2.1.1	Provide video clips for a pre-determined length of time before event, during event, Post event with EOC-DC providing increments per view
Digital Video Management		

Digital Video Management		
Digital Video Management	2.2 Retention shall be based on asset being monitored with pre-defined durations as defined by EOC-DC Management and by MiCMDB Business Criticality type	Differentiate between criticality levels of High, Medium and Low
Digital Video Management	3	Resolution degradation over time for storage purposes
Digital Video Management		Lengths of video clip retention
Digital Video Management		Maximum Length of available retention standard
Digital Video Management	3.0.1	
Digital Video Management	4.0 Capture Locations and view definitions	
Digital Video Management	4.1 All device placements shall be reviewed frequently for view quality	
Digital Video Management	4.1.1 Twice Yearly	Determinate upon Business Criticality of camera capture view
Digital Video Management	4.1.2 Annually	All are reviewed annually
Digital Video Management	4.2 All current views shall be reviewed for:	<ul style="list-style-type: none"> Content of view location of device for best viewing Activation levels as defined 1.a and 1.b Areas shall be assessed for identification/elimination of dark paths and blind spots (paths where you can travel with no camera exposure) 200% coverage is a minimum
Digital Video Management		
Digital Video Management		
Digital Video Management		
Digital Video Management		
Digital Video Management	5.0 Issue Management	
Digital Video Management	5.1 Clip retrieval follows the following	
Digital Video Management	5.1.1 Human Resources Requested	

Digital Video Management	5.1.1.1	Follow all associated policies, standards and procedures
Digital Video Management	5.1.2 EOC-DC Business process management requested	
Digital Video Management	5.1.2.1	Management of clips shall be at the discretion of EOC-DC Facility management or their designee
Digital Video Management		
Digital Video Management	6.0 External system integrations	
Digital Video Management	6.1	Outage/Tampering/Quality of Service (QOS) Event management must report to EOC-DC via SNMP Traps from smart devices and/or Remedy for alarm ticketing
Digital Video Management	7.0 Reporting	
Digital Video Management	7.1 Formatting	
Digital Video Management	7.1.1 All reports are to be generated showing the following information	<ul style="list-style-type: none"> • Time/Date stamped • Who accessed including attempts to access • Devices impacted by previous bullet • Previous/Current value if settings were changed
Digital Video Management		
Digital Video Management		
Digital Video Management		
Digital Video Management		
Digital Video Management	7.2 Frequency of Report Delivery	
Digital Video Management	7.2.1 Monthly	First calendar day the Month
Digital Video Management	7.2.2 Quarterly	Summary of current month including the previous 2 months
Digital Video Management	7.2.3 Annually	Summary of the 4 quarter reports
Digital Video Management	7.2.4 Exclusions	Human Resources (HR) Clip Request
Digital Video Management	8.0 Clip retrieval	
Digital Video Management	8.1 EOC-DC View/Export	
Digital Video Management	8.1.1	Functionality that allows the State view on demand clips
Digital Video Management	8.1.2	Capability of 24/7/365 Live Streaming for onsite staff to maintain situational monitoring

Digital Video Management	8.2 VENDOR Access	
Digital Video Management	9.0 SSP Information	
Digital Video Management	9.1 Common Control	Must provide all common controls for inclusion into Risk Assessment
Digital Video Management	10.0 Camera Status	
Digital Video Management	0.0 Data Capture	
Digital Video Management	1.0 Motion Capture	Must be able to capture within pre-defined areas within field of view (blank out areas where motion capture is not desired)
Digital Video Management		Provide alarming at time of event for by a Remedy ticket for unexpected motion detection per location EOC-DC pre-defined area requirements
Digital Video Management		
Digital Video Management		
Digital Video Management	2.0 Partial field of vision management (Blocked areas)	As provided by areas pre-defined by management of location parts of the view will require that blocking of incidental view capture must be available.
Digital Video Management		
Digital Video Management		
Digital Video Management	3.0 Resolution degradation over time for storage purposes	Lengths of video clip retention and phased degradation is at EOC-DC Management discretion
Digital Video Management		
Digital Video Management		
Digital Video Management	1.1 Personal Computer (PC) Operating System (OS) level	Windows 10 or higher is recommended
Digital Video Management		
Digital Video Management		
Digital Video Management	1.2 Browser Type	Microsoft Edge / Chrome / Firefox or above is recommended as the web portal
Digital Video Management		
Digital Video Management		
Digital Video Management	1.3 Connection Type	Users must have an internet browser to use the system
Digital Video Management		
Digital Video Management		
Digital Video Management	3 Security Posture	

Digital Video Management	3.1 Access controls	
Digital Video Management		
Digital Video Management	3.1.1	All data access is to be managed by non-self-signed SSL Certificate with ID/PW
Digital Video Management		
Digital Video Management	3.2 Management application user access	
Digital Video Management	3.2.1 Group Management	
Digital Video Management		
Digital Video Management	3.2.1.1	All access levels are to be managed by LDAPS AD groups and follow the DTMB-0161 and DTMB-927 access process
Digital Video Management		
Digital Video Management	3.2.1.2 Levels of access by LDAPS Group (EOC-DC_DVM_<Group Name>)	
Digital Video Management		EOC-DC have the ability to manage the lesser pre-defined roles as follows:
Digital Video Management		Has the ability to manipulate pre-defined views available to the Power User and Read Only roles.
Digital Video Management	3.2.1.2.1	Power User:
Digital Video Management		Has the ability to manipulate pan tilt zoom (PTZ) devices with stop and start recording
Digital Video Management		Read Only_<Location>:
Digital Video Management		Access to view only pre-defined views as designated by ID and location
Digital Video Management	4 Technology Management	
Digital Video Management		Security Vulnerabilities must be remediated by the vendor in a timely manner as part of the Contract
Digital Video Management	4.1 Software Management	Software updates to new version levels costing must be included as part of the Contract and included in final application management costing
Digital Video Management		Planned software updates and patches of application and modules must follow State of Michigan RFC process with EOC-DC being an impacted party

Digital Video Management	4.2 Camera Status	Camera Event Alarming must be presented through Nlyte Energy Optimizer (NEO) Alarming Required NEO Alarm Licenses need to be identified and provided
Digital Video Management	4.2.1 Alarm Types	Camera Tamper Camera Internal Status
Nlyte Energy Optimizer NEO Monitoring	Business Req. No.	Detailed Business Requirement Description
Nlyte Energy Optimizer NEO Monitoring	0.0 Disaster Recovery	
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	0.0.1 Loss of Power to Modules	
Nlyte Energy Optimizer NEO Monitoring	0.0.1.1	Modules
Nlyte Energy Optimizer NEO Monitoring	0.0.1.1.1	Main Application should provide an alarm of loss of communication
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	0.0.1.1.2	All self-powered modules need to maintain data until communication is restored
Nlyte Energy Optimizer NEO Monitoring	0.0.1.2	Communication methods are <ul style="list-style-type: none"> • Simple Mail Transfer Protocol (SMTP) (email/text) • Remedy ticket update/notification to follow
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		

Nlyte Energy Optimizer NEO Monitoring	0.0.1.3	Time/Date of event occurrence
Nlyte Energy Optimizer NEO Monitoring	0.0.1.5	Time/Date of validated return to operation (return to Normal)
Nlyte Energy Optimizer NEO Monitoring	0.0.2.0 Data Back Entry	
Nlyte Energy Optimizer NEO Monitoring	0.0.2.1	Paper Data Entry must be up loadable via a spread sheet where entry data is captured during outages
Nlyte Energy Optimizer NEO Monitoring	0.0.2.1.1	Power User is the lowest level for this type of access
Nlyte Energy Optimizer NEO Monitoring	1 Security Posture	
Nlyte Energy Optimizer NEO Monitoring	1.1 Access controls	
Nlyte Energy Optimizer NEO Monitoring	1.1.1	All access is to be managed by
Nlyte Energy Optimizer NEO Monitoring		<ul style="list-style-type: none"> • AD Group controlled for each level of access to be granted
Nlyte Energy Optimizer NEO Monitoring		<ul style="list-style-type: none"> ○ Service Account (full admin rights)
Nlyte Energy Optimizer NEO Monitoring		<ul style="list-style-type: none"> ○ Application Admin
Nlyte Energy Optimizer NEO Monitoring		<ul style="list-style-type: none"> ○ Power User
Nlyte Energy Optimizer NEO Monitoring		<ul style="list-style-type: none"> ○ Read Only
Nlyte Energy Optimizer NEO Monitoring	1.1.1.1	Access to client consoles and/or pre-determined designed view is to be managed via LDAPS AD Group(s)

Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	1.1.1.2	All access to views within EOC-DC managed locations are to be pre-determined by the following:
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	1.1.1.2.1	<ul style="list-style-type: none"> • Job description for view access • All Access is approved by EOC-DC Management • Active Directory (AD) Group managed
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	2	
Nlyte Energy Optimizer NEO Monitoring	Data Retention	
Nlyte Energy Optimizer NEO Monitoring	2.1	
Nlyte Energy Optimizer NEO Monitoring	All base alarm data is to be managed as follows:	
Nlyte Energy Optimizer NEO Monitoring	2.1.1	Provide reports for selected periods of time for event tracking
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		

Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	3.0 Issue Management	
Nlyte Energy Optimizer NEO Monitoring	3.1 Change History retrieval	
Nlyte Energy Optimizer NEO Monitoring	3.1.2 EOC-DC Business process management requested	
Nlyte Energy Optimizer NEO Monitoring	3.1.2.1	Management of reports shall be at the discretion of EOC-DC Facility management or their designee
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	4.0 External system integrations	
Nlyte Energy Optimizer NEO Monitoring	4.1	External integrations are to be managed by EOC-DC management and corresponding MOU's with data connections that are application specific
Nlyte Energy Optimizer NEO Monitoring	5.0 Reporting	
Nlyte Energy Optimizer NEO Monitoring	5.1 Formatting	
Nlyte Energy Optimizer NEO Monitoring	5.1.1 All reports are to be generated showing the following information	<ul style="list-style-type: none"> • Time/Date stamped
Nlyte Energy Optimizer NEO Monitoring		<ul style="list-style-type: none"> • Who accessed including attempts to access
Nlyte Energy Optimizer NEO Monitoring		<ul style="list-style-type: none"> • Devices impacted by previous bullet
Nlyte Energy Optimizer NEO Monitoring		<ul style="list-style-type: none"> • Previous/Current value if settings were changed for changes

Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	5.2 Frequency of Report Delivery	
Nlyte Energy Optimizer NEO Monitoring	5.2.1 Monthly	First calendar day the Month
Nlyte Energy Optimizer NEO Monitoring	5.2.2 Quarterly	Summary of current month including the previous 2 months
Nlyte Energy Optimizer NEO Monitoring	5.2.3 Annually	Summary of the 4 quarter reports
Nlyte Energy Optimizer NEO Monitoring	5.2.4 Exclusions	HR Request
Nlyte Energy Optimizer NEO Monitoring	6.0 Data retrieval	
Nlyte Energy Optimizer NEO Monitoring	6.1 EOC-DC View/Export	
Nlyte Energy Optimizer NEO Monitoring	6.1.1	EOC-DC reserves the right to view/retrieve on demand reports
Nlyte Energy Optimizer NEO Monitoring	6.1.2	Capability of 24/7/365 availability for onsite staff to maintain situational monitoring
Nlyte Energy Optimizer NEO Monitoring	7.0 SSP Information	
Nlyte Energy Optimizer NEO Monitoring	7.1 Common Control	Must provide all common controls for inclusion into Risk Assessment
Nlyte Energy Optimizer NEO Monitoring	0.0 Data Retention	

Nlyte Energy Optimizer NEO Monitoring	1.0 Data Capture	<p>The purpose of this section is to outline the processes for Data Capture</p> <ul style="list-style-type: none"> Data capture is performed upon input of an event Data capture is saved at a certain level before application software Data will be available at the module level for Disaster Recovery purposes
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	1.1 Loss of Communication	<p>The purpose of this section is to describe process for in module data capture during a Loss of Communication Event</p> <ul style="list-style-type: none"> All data is to be stored in the highest-level module where communication is maintained
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	1.2 Data Restoration after Loss of Communication	<p>The purpose of this section is to describe process for restoration of saved event data that occurred during an outage</p> <ul style="list-style-type: none"> Upon reconnection of communication data is sent to main application in such a manor where the main application is not overwhelmed where new current event data is ignored.
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		

Nlyte Energy Optimizer NEO Monitoring	2.0 Application Access	The purpose of this section is to describe the different levels of access.
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	2.1 Application User Access	<ul style="list-style-type: none"> • Application Access (API, Application, SQL and Service Accounts) is to be role based with the following access levels <ul style="list-style-type: none"> ○ Service Account ○ Application Administrator ○ Application Power User ○ Application Read only user ○ SQL Access Read only User • SQL Read only access must be Service Account controlled •
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	2.2 Application Data Sharing	<ul style="list-style-type: none"> • SQL Read only access must be Service Account controlled • All API parameters must be provided
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		

Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	2.2.1 External SQL	<ul style="list-style-type: none"> • The Data Base must be compatible with other Micro Soft SQL products • A map of the Data Base including but not limited to the following <ul style="list-style-type: none"> ○ Table Names ○ Table field types and lengths ○ Table field relationships ○ Table field logical build (the “math” behind a concatenated or other logical function that was performed upon it)
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	2.2.2 Locations of Truth	<ul style="list-style-type: none"> • Asset location of truth must be provided by NAO
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	2.2.3 Event Alarm Management	
Nlyte Energy Optimizer NEO Monitoring	2.2.3.1 Alarm Management by external Application(s)	<ul style="list-style-type: none"> • Event Alarming must be of SNMP trap and MIB in nature

Nlyte Energy Optimizer NEO Monitoring		<ul style="list-style-type: none"> Event Alarming must be compatible with Nlyte NEO functionality.
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	2.2.3.2 Alarm Management Local to Application(s)	<ul style="list-style-type: none"> All Event Alarms must be maintained internally to the application
Nlyte Energy Optimizer NEO Monitoring		<ul style="list-style-type: none"> Application must have the ability to act as main event alarm notification portal
Nlyte Energy Optimizer NEO Monitoring		<ul style="list-style-type: none"> Additional NEO alarm points will need to be identified and proper licenses need to be included
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	3.0 Integrations	Application must be recognized by Nlyte as a recognized partner for application integrations for NAO, NEO and Nlyte Command functionality to be maintained
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	4.0 Data Capture	This section describes the different types of data capture methods and sensor types
Nlyte Energy Optimizer NEO Monitoring	4.1 Normally Open / Normally Closed	
Nlyte Energy Optimizer NEO Monitoring		Read Normally Open / Normally Closed Contact data
Nlyte Energy Optimizer NEO Monitoring		

Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	4.2 Analog and Digital data capture	<ul style="list-style-type: none"> Analog Data: convert analog data into a digital value for event management Digital Data: To be able to manage digital data streams and provide event management such as the following: BACnet, MODBUS+, Serial Data Streams...
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	4.3 Sensor Types	The following are the different sensor communication types
Nlyte Energy Optimizer NEO Monitoring	4.3.1 Analog Data	<p>The ability to read analog data inputs of various types</p> <p>Additional NEO alarm points will need to be identified and proper licenses need to be included</p>
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	4.3.2 Binary Data	<p>The ability to read binary data inputs of various types</p> <p>Additional NEO alarm points will need to be identified and proper licenses need to be included</p>
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		

Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	4.3.2.1 Wi-Fi	<ul style="list-style-type: none"> · All Wi-Fi must have the following parameters: <ul style="list-style-type: none"> o Must adhere to State of Michigan Security Protocols o Must be compatible of diverse power o Additional NEO alarm points will need to be identified and proper licenses need to be included
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	4.3.2.2 Serial Data Connection	Must be compatible with all standard Seral Data Streams and with Vertiv Velocity AC Control protocols
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	4.4 Module self-diagnosis	All modules must provide a self-diagnosis of fault state that will impact it's functionality and provide alarming and processes for remediation of internal faults
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		

Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	1.1 Personal Computer (PC) Operating System (OS) level	Windows 10 or higher is recommended
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	1.2 Browser Type	Microsoft Edge / Chrome / Firefox or above is recommended as the web portal
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	1.3 Connection Type	Users must have an internet browser to use the system
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	3 Security Posture	
Nlyte Energy Optimizer NEO Monitoring	3.1 Access controls	
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	3.1.1	All data access is to be managed by non-self-signed SSL Certificate with ID/PW
Nlyte Energy Optimizer NEO Monitoring		

Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	3.2 Management application user access	
Nlyte Energy Optimizer NEO Monitoring	3.2.1 Group Management	
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	3.2.1.1	All access levels are to be managed by LDAPS AD groups and follow the DTMB-0161 and DTMB-927 access process
Nlyte Energy Optimizer NEO Monitoring		
Nlyte Energy Optimizer NEO Monitoring	3.2.1.2 Levels of access by LDAPS Group (EOC-DC_DVM_<Group Name>)	
Nlyte Energy Optimizer NEO Monitoring		EOC-DC have the ability to manage the lesser pre-defined roles as follows:
Nlyte Energy Optimizer NEO Monitoring		Has the ability to manipulate pre-defined views available to the Power User and Read Only roles.
Nlyte Energy Optimizer NEO Monitoring	3.2.1.2.1	Power User:
Nlyte Energy Optimizer NEO Monitoring		Has the ability to Access various modules via LDAP/LAN connections for configuration and patch installation and configuration.
Nlyte Energy Optimizer NEO Monitoring		Read Only_<Location>:
Nlyte Energy Optimizer NEO Monitoring		Access to view only pre-defined views as designated by ID and location

Nlyte Energy Optimizer NEO Monitoring	4 Technology Management	<ul style="list-style-type: none"> Security Vulnerabilities for Application and Modules must be remediated by the vendor in a timely manner as part of the Contract Planned software updates and patches of application and modules must follow State of Michigan RFC process with EOC-DC being an impacted party
Nlyte Energy Optimizer NEO Monitoring		
Rack Lock Management	Business Req. No.	Detailed Business Requirement Description
Rack Lock Management	1	Control Software Security Posture
Rack Lock Management	1.1.	Loss of Power / Connectivity
Rack Lock Management	1.1.1.	Data Retention
Rack Lock Management	1.1.1.1.	Lock Level
Rack Lock Management	1.1.1.1.1.	Locks shall retain the following information
Rack Lock Management	1.1.1.1.1.1.	Type of access device used
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.1.1.1.1.2.	Unique access device identifier
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.1.1.1.1.3.	Date/Time of event
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.1.1.1.1.4.	Retain last programmed profile for access
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.1.1.2.	Room Reporting Layer
Rack Lock Management	1.1.1.2.1.	Able to upload the available data from locks upon power resumption
Rack Lock Management		

Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.1.1.2.2.	Store last programmed states if connectivity above is lost
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.1.1.2.3.	Upon connectivity restoration upload activity to main application
Rack Lock Management		
Rack Lock Management	1.1.1.3.	Application Layer
Rack Lock Management		
Rack Lock Management	1.1.1.3.1.	Alarm for loss of connectivity anywhere along the lock communication path
Rack Lock Management		
Rack Lock Management	1.1.1.3.2.	Alarm for actionable activity once communication is restored
Rack Lock Management		
Rack Lock Management	1.1.1.4.	Upon power resumption, all data is automatically uploaded with testing for alarm conditions having occurred
Rack Lock Management		
Rack Lock Management	1.1.2.	Door States upon Power Loss
Rack Lock Management		
Rack Lock Management	1.1.2.1.	At Cabinet
Rack Lock Management		

Rack Lock Management		
Rack Lock Management	1.1.2.1.1.	Failure States
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.1.2.1.1.1.	Lock remains in last state
Rack Lock Management		
Rack Lock Management	1.1.2.1.1.1.1.	If cabinet door locked it remains locked
Rack Lock Management		
Rack Lock Management	1.1.2.1.1.1.2.	If cabinet door is unlock it remains unlocked
Rack Lock Management		
Rack Lock Management	1.1.2.1.1.2.	Master key access to open lock
Rack Lock Management		
Rack Lock Management	1.1.2.1.1.2.1.	Physical or powered key to change locked state of cabinet Door
Rack Lock Management		
Rack Lock Management	1.1.2.1.1.3.	Alarming for low battery (if applicable)
Rack Lock Management		
Rack Lock Management	1.1.2.2.	At Management Infrastructure
Rack Lock Management		
Rack Lock Management	1.1.2.2.1.	Loss of Network
Rack Lock Management		
Rack Lock Management	1.1.2.2.2.	Devices will auto re-establish connectivity without manual intervention upon return to power
Rack Lock Management		
Rack Lock Management		

Rack Lock Management	1.2.	User Access
Rack Lock Management	1.2.1.	All user access is to be provided by
Rack Lock Management	1.2.1.1.	AD Group(s)
Rack Lock Management		
Rack Lock Management	1.2.1.1.1.	Have the ability to manage application
Rack Lock Management	1.2.1.1.1.1.	Access to the application (log on)
Rack Lock Management	1.2.1.1.1.2.	Granular application role based function control
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.2.1.2.	SLDAP authentication
Rack Lock Management	1.2.1.2.1.	To provide multi factor role based authentication
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.2.2.	Supported User Access Types
Rack Lock Management	1.2.2.1.	Login
Rack Lock Management		
Rack Lock Management	1.2.2.1.1.	Read Only
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.2.2.1.2.	Power User
Rack Lock Management		

Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.2.2.1.3.	Application Administrator
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.2.2.1.4.	Service Accounts
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.2.2.1.4.1.	Application
Rack Lock Management	1.2.2.1.4.2.	Integration
Rack Lock Management	1.2.2.1.5.	Screen viewer and functionality granularity
Rack Lock Management		
Rack Lock Management	1.2.2.1.5.1.	All access is governed by AD Group
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.2.2.1.5.1.1.	Similar AD Groups will have determinable access as governed by least access
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.3.	Provide visit based access as managed by an external reservation system
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.3.1.	Provides the following functionality
Rack Lock Management		
Rack Lock Management	1.3.1.1.	Asset owner Role/Group based access
Rack Lock Management		

Rack Lock Management	1.3.1.2.	Asset associated access
Rack Lock Management	1.3.1.2.1.	Allows for access to other cabinets per data provided by CMDB for external connection access (power and network connections)
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.4.	Reporting requirements
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.4.1.	Access attempts
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.4.1.1.	Successful and failed access attempt reports
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.4.1.1.1.	Date/Time stamped
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.4.1.1.2.	Who attempted if Personal Identifiable Information (PII) data available
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.4.1.1.3.	Export data directly from lock mechanism if desired
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.4.2.	Ad hoc reporting methods
Rack Lock Management	1.4.3.	Active Directory Group Management

Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.4.3.1.	Management of software for views and accessing management console
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.4.4.	Format and frequency
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.4.4.1.	Calendared automated reporting
Rack Lock Management		
Rack Lock Management	1.5.	External integrations
Rack Lock Management	1.5.1.	Remedy
Rack Lock Management		
Rack Lock Management	1.5.1.1.	External Alarming with Ticketing (Remedy) for communication of events
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.1.2.	Types of alarming for ticket generation
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.1.2.1.	Tampering (unplanned door opening)
Rack Lock Management		

Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.1.2.2.	Loitering
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.1.2.3.	Motion depending upon the area criticality
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.2.	DCIM Nlyte Energy Optimizer (NEO)
Rack Lock Management		
Rack Lock Management	1.5.2.1.	SNMP traps for alarm event application licenses by lock module.
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.2.1.1.	May include Remedy ticket auto generation
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.3.	DCIM Nlyte Asset Optimizer (NAO)
Rack Lock Management		
Rack Lock Management	1.5.3.1.	Asset ONLY location of truth
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.3.2.	Provide asset interconnections for multiple cabinet management.
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		

Rack Lock Management	1.5.4.	DVM Tool (TBD)
Rack Lock Management		
Rack Lock Management	1.5.4.1.	Event of forced entry to trigger automatic video recording of event
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.5.	Reservation system (TBD)
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.5.1.	Activation of controlled entry must follow:
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.5.1.1.	Enable specified entry during pre-arranged reservation time with +/-
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.5.1.2.	Utilizing data from NAO must suppress alarming for requested asset access and time
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.5.1.3.	Will allow for multiple parties to have access concurrent cabinets
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.5.6.	Motion Capture (TBD)
Rack Lock Management	1.5.6.1.	

Rack Lock Management		
Rack Lock Management		Alarm management between door activation (selective or general) must be recognizable to a Digital Management System for Video Capture of access attempts.
Rack Lock Management		
Rack Lock Management	1.6.	Alarms
Rack Lock Management		
Rack Lock Management	1.6.1.	All alarms provided to EOC-DC Management for the following for each occurrence at the time of occurrence:
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.6.2.	Communication method is to include pertinent information and can utilize the following methods:
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.6.2.1.	Email / Text
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.6.2.2.	SNMP Trap(s)
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.6.2.3.	Remedy Incident Ticket Generation
Rack Lock Management		
Rack Lock Management	1.6.3.	Management Infrastructure
Rack Lock Management	1.6.3.1.	Main Application alarms
Rack Lock Management	1.6.3.2.	No loss of data shall occur

Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.6.4.	Functional Alarms (All Alarms must be managed by Nlyte Energy Optimizer and the associated licenses must be accounted for notifications)
Rack Lock Management		
Rack Lock Management	1.6.4.1.	Upon attempted access
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.6.4.1.1.	Where selected
Rack Lock Management		
Rack Lock Management	1.6.4.1.2.	Multiple door attempts
Rack Lock Management		
Rack Lock Management	1.6.4.1.2.1.	Fishing for rogue access
Rack Lock Management		
Rack Lock Management	1.6.5.2.	Door left ajar
Rack Lock Management		
Rack Lock Management	1.6.5.3.	Loss of door ajar sensor
Rack Lock Management		

Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.7.	Vulnerability Management
Rack Lock Management		
Rack Lock Management	1.7.1.	All vulnerabilities must be remediated per the State of Michigan Standards and Procedures
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.7.1.1.	Current testing (but not limited too)
Rack Lock Management		
Rack Lock Management	1.7.1.1.1.	Operating System (OS) interactive vulnerability(s) (Tenable)
Rack Lock Management		
Rack Lock Management	1.7.1.1.2.	Application function call vulnerability(s)
Rack Lock Management		
Rack Lock Management	1.7.1.1.2.1.	Internal to the application (App Scan)
Rack Lock Management		
Rack Lock Management	1.7.1.1.2.2.	External to the application with middleware (SADLC Scan)
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		

Rack Lock Management	2	Technology to be provided
Rack Lock Management		
Rack Lock Management	2.1.	Provide cabinet assessments with the following information
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	2.1.1.	Types of mechanical interfaces of the locks by cabinet type to be provided
Rack Lock Management		
Rack Lock Management	2.1.2.	Types of lock activators
Rack Lock Management		
Rack Lock Management	2.1.2.1.	Electronic Card
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	2.1.2.2.	Personnel Identification Number (PIN)
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	2.1.2.3.	Biometric
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	2.1.2.4.	Master Key
Rack Lock Management		
Rack Lock Management	2.2.	

Rack Lock Management		
Rack Lock Management		Provide drawings showing field of coverage for the areas requested to be managed with EOC-DC Management approval
Rack Lock Management		
Rack Lock Management	3	Training
Rack Lock Management	3.1.	Training in the following will be provided
Rack Lock Management		
Rack Lock Management	3.1.1.	Application hardware and software management
Rack Lock Management		
Rack Lock Management	3.1.2.	User Training
Rack Lock Management		
Rack Lock Management	3.1.2.1.	User training is segregated by job type
Rack Lock Management		
Rack Lock Management	3.1.2.1.1.	Example
Rack Lock Management	3.1.2.1.1.1.	Read only
Rack Lock Management	3.1.2.1.1.2.	Power User
Rack Lock Management	3.1.2.1.1.3.	Application Administration
Rack Lock Management	4	Technology Refresh
Rack Lock Management		
Rack Lock Management	4.1.	Software updates are part of the maintenance costing
Rack Lock Management		
Rack Lock Management	4.2.	Industrial Services will be engaged in the installation of new software

Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	4.3.	End of Life notifications
Rack Lock Management		
Rack Lock Management		
Rack Lock Management	0.0 Data Capture	
Rack Lock Management		Must be able to capture within pre-defined areas within field of view (blank out areas where motion capture is not desired)
Rack Lock Management	1.0 Activation Attempts	Provide alarming at time of event for by a Remedy ticket for unexpected motion detection per location EOC-DC pre-defined area requirements
Rack Lock Management		
Rack Lock Management	2.0 Partial area access controls (Blocked areas)	As provided by areas pre-defined by management of locations where access blocking of incidental view capture must be available.
Rack Lock Management		
Rack Lock Management	3.0 Data purging due to timer activated	Lengths of access attempts retention and phased removal is at EOC-DC Management discretion
Rack Lock Management		
Rack Lock Management	4.0 All out-of-scope access attempts must be recorded	All attempts even if the access alarms have been silenced must be logged.
Rack Lock Management		
Rack Lock Management	5.0 By site, emergency remote lock/unlock	Emergency lock/unlock must be provided on a cabinet-by-cabinet basis or group
Rack Lock Management		

Rack Lock Management		
Rack Lock Management		
Rack Lock Management	1.1 Personal Computer (PC) Operating System (OS) level	Windows 10 or higher is recommended
Rack Lock Management		
Rack Lock Management	1.2 Browser Type	Microsoft Edge / Chrome / Firefox or above is recommended as the web portal
Rack Lock Management		
Rack Lock Management	1.3 Connection Type	Users must have an internet browser to use the system
Rack Lock Management		
Rack Lock Management	3 Security Posture	
Rack Lock Management	3.1 Access controls	
Rack Lock Management	3.1.1	All data access is to be managed by non-self-signed SSL Certificate with ID/PW
Rack Lock Management		
Rack Lock Management	3.2 Management application user access	
Rack Lock Management	3.2.1 Group Management	
Rack Lock Management	3.2.1.1	All access levels are to be managed by LDAPS AD groups and follow the DTMB-0161 and DTMB-927 access process
Rack Lock Management		
Rack Lock Management	3.2.1.2 Levels of access by LDAPS Group (EOC-DC_DVM_<Group Name>)	
Rack Lock Management	3.2.1.2.1	EOC-DC to have the ability to manage the lesser pre-defined roles as follows: Has the ability to manipulate pre-defined views available to the Power User and Read Only roles.
Rack Lock Management		

Rack Lock Management		Power User:
Rack Lock Management		Read Only_<Location>:
Rack Lock Management		Access to view only pre-defined views as designated by ID and location
Rack Lock Management	4 Technology Management	Security Vulnerabilities of software for application and all modules must be remediated by the vendor in a timely manner as part of the Contract
Rack Lock Management		Software updates to new version levels costing must be included as part of the Contract and included in final application management costing
Rack Lock Management		Planned software updates and patches of application and modules must follow State of Michigan RFC process with EOC-DC being an impacted party
RFID Asset Management	Business Req. No.	Detailed Business Requirement Description
RFID Asset Management	1	Disaster Recover
RFID Asset Management	1.1.	Loss of Power
RFID Asset Management	1.1.1.	
RFID Asset Management	1.2.	Loss of Communication
RFID Asset Management	1.2.1.	In the event of a loss of communication with the management server(s) but the capture device remains powered local to the capture device storage shall be utilized with uploading capability once communication is reestablished with Management Server(s)
RFID Asset Management	1.2.2.	Outage/Tampering/QOS Event management must report to EOC-DC via SNMP Traps or internal loss of communication alarms from smart device and/or Remedy for alarm ticketing
RFID Asset Management	2	Security
RFID Asset Management	2.1.	Access Control
RFID Asset Management	2.1.1.	Access to client consoles and/or pre-determined designed view is to be managed via SLDAP AD Group(s)
RFID Asset Management		
RFID Asset Management	2.1.2.	

RFID Asset Management		All access to views within EOC-DC managed locations are to be pre-determined by the following:
RFID Asset Management		
RFID Asset Management		
RFID Asset Management	2.1.2.1.	Job description for application access
RFID Asset Management		
RFID Asset Management		
RFID Asset Management		
RFID Asset Management	2.1.2.3.	All Access is approved by EOC-DC Management ticket number stored and searchable
RFID Asset Management		
RFID Asset Management	3	Data Retention
RFID Asset Management		
RFID Asset Management	3.1.	Data is to be retained for the life cycle of the application
RFID Asset Management		
RFID Asset Management		
RFID Asset Management	3.1.1.	Must be migratable between current and all future versions
RFID Asset Management		
RFID Asset Management		
RFID Asset Management	3.1.2.	Data is not be removable from the system but can be rendered invisible but able to be retrieved by administrator only
RFID Asset Management		
RFID Asset Management	4	Data Capture
RFID Asset Management		Data is to be captured by the following physical locations:
RFID Asset Management		Cabinet Level
RFID Asset Management	4.1.	Floor/Room Level
RFID Asset Management		Building
RFID Asset Management	5	Reporting
RFID Asset Management	5.1.	Types

RFID Asset Management		
RFID Asset Management	5.1.1.	All reports are to be generated showing the following information
RFID Asset Management		
RFID Asset Management		
RFID Asset Management	5.1.1.1.	Time/Date stamped
RFID Asset Management		
RFID Asset Management		
RFID Asset Management	5.1.1.2.	Who accessed including attempts to access
RFID Asset Management		
RFID Asset Management		
RFID Asset Management	5.1.1.3.	Devices impacted by previous bullet
RFID Asset Management		
RFID Asset Management		
RFID Asset Management	5.1.1.4.	Previous/Current value if settings were changed
RFID Asset Management		
RFID Asset Management	5.2.	Automation
RFID Asset Management		Automated reports must be sent:
RFID Asset Management	5.2.1.	<ul style="list-style-type: none"> • Monthly • Quarterly • Annually
RFID Asset Management		
RFID Asset Management	5.3.	EOC-DC reserves the right to view/retrieve on demand
RFID Asset Management		
RFID Asset Management	6	External Integrations

RFID Asset Management	6.1.	Remedy
RFID Asset Management		
RFID Asset Management	6.1.1.	High criticality devices have auto ticket generation
RFID Asset Management		
RFID Asset Management	6.2.	DCIM Nlyte Energy Optimizer (NEO)
RFID Asset Management	6.2.1.	Integration with SMTP alarming including alarm point licenses
RFID Asset Management		
RFID Asset Management	6.3.	DCIM Nlyte Asset Optimizer (NAO)
RFID Asset Management		
RFID Asset Management	6.3.1.	<ul style="list-style-type: none"> Application integration including module licenses
RFID Asset Management		
RFID Asset Management	6.4.	DVM Tool (TBD)
RFID Asset Management		
RFID Asset Management	6.5.	Reservation System (TBD)
RFID Asset Management		
RFID Asset Management	7	System Security Profile (SSP)
RFID Asset Management	7.1.	Provide National Institute of Standards and Technology (NIST) moderate risk assessment control responses
RFID Asset Management	8	Auditing
RFID Asset Management	8.1.	Reports
RFID Asset Management		
RFID Asset Management	8.1.1.	Virtual Audits of pings from tags in the environments
RFID Asset Management		
RFID Asset Management	8.2.	Manual Auditing
RFID Asset Management	8.3.	Processing

RFID Asset Management		
RFID Asset Management	8.3.1.	Automated calendar instituted virtual audit
RFID Asset Management		
RFID Asset Management		
RFID Asset Management	8.3.2.	Manually created-configured/automated audit
RFID Asset Management		
RFID Asset Management	0.0 Data Capture	
RFID Asset Management		Must be able to capture within pre-defined areas where motion capture is desired
RFID Asset Management	1.0 Motion Capture	Provide alarming at time of event for by a Remedy ticket for unexpected motion detection per location EOC-DC pre-defined area requirements
RFID Asset Management		
RFID Asset Management	2.0 Tag movement of room edge detection	Provide movement tracking/alarming of asset(s) location(s) as they move through and to/from monitored locations
RFID Asset Management		
RFID Asset Management	3.0 Auditing	Demonstrate active auditing of devices in their chosen location
RFID Asset Management		
RFID Asset Management	1.1 Personal Computer (PC) Operating System (OS) level	Windows 10 or higher is recommended
RFID Asset Management		
RFID Asset Management	1.2 Browser Type	Microsoft Edge / Chrome / Firefox or above is recommended as the web portal
RFID Asset Management		
RFID Asset Management	1.3 Connection Type	Users must have an internet browser to use the system
RFID Asset Management		
RFID Asset Management	3 Security Posture	
RFID Asset Management	3.1 Access controls	

RFID Asset Management		
RFID Asset Management	3.1.1	All data access is to be managed by non-self-signed SSL Certificate with ID/PW
RFID Asset Management		
RFID Asset Management	3.2 Management application user access	
RFID Asset Management	3.2.1 Group Management	
RFID Asset Management		
RFID Asset Management	3.2.1.1	All access levels are to be managed by LDAPS AD groups and follow the DTMB-0161 and DTMB-927 access process
RFID Asset Management		
RFID Asset Management	3.2.1.2 Levels of access by LDAPS Group (EOC-DC_DVM_<Group Name>)	
RFID Asset Management		EOC-DC have the ability to manage the lesser pre-defined roles as follows:
RFID Asset Management	3.2.1.2.1	Has the ability to manipulate pre-defined views available to the Power User and Read Only roles.
RFID Asset Management		Power User:
RFID Asset Management		Software updates to application and modules of new version levels costing must be included as part of the Contract and included in final application management costing
RFID Asset Management		Planned software updates and patches of application and modules must follow State of Michigan RFC process with EOC-DC being an impacted party
Visitor Management	Business Req. No.	Detailed Business Requirement Description
Visitor Management	0.0 Disaster Recovery	
Visitor Management	0.0.1	Loss of Power to Signature pad
Visitor Management	0.0.1.1	Signature pad.
Visitor Management	0.0.1.1.1	Must become active at reboot with no user interaction. Auto Discovered

Visitor Management	0.0.1.1.2	Must be accessible by any login location by individual with certain rights (example, reservation is started in one location with remote location providing sign on)
Visitor Management	0.0.1.2	Communication methods are
Visitor Management		<ul style="list-style-type: none"> • Simple Mail Transfer Protocol (SMTP) (email/text) • Remedy ticket update/notification to follow
Visitor Management	0.0.1.3	Time/Date of event occurrence
Visitor Management	0.0.1.4	Remedy Incident / Emergency RFC number shall be validated as active at time of reservation submission
Visitor Management	0.0.1.5	Estimated Time of Return to Operation (dependent upon the type of alarm provided)
Visitor Management	0.0.1.6	Time/Date of validated return to operation (return to Normal)
Visitor Management	0.0.1.7	Post mortem Root Cause Analysis (RCA) with results documented as following
Visitor Management	0.0.1.7.1	Providing all steps and communication activity for issue remediation
Visitor Management	0.0.1.8	Current and future activity to eliminate the re-occurrence of event
Visitor Management	0.0.1.9	Sign off from EOC-DC Management of event conclusion and resolution
Visitor Management	0.0.2.0 Data Back Entry	
Visitor Management	0.0.2.1	Paper Data Entry must be up loadable via a spread sheet where entry data is captured during outages
Visitor Management	0.0.2.1.1	Power User is the lowest level for this type of access
Visitor Management	1 Security Posture	
Visitor Management	1.1 Access controls	
Visitor Management	1.1.1	All access is to be managed by
Visitor Management		<ul style="list-style-type: none"> • location, • highest access allowed and • residents must have automated approval
Visitor Management		
Visitor Management		

Visitor Management		<ul style="list-style-type: none"> • tracking of with Expiration Timers: <ul style="list-style-type: none"> ○ Items provided <ul style="list-style-type: none"> ▪ Badges ▪ Keys ▪ Tools ○ Perishable Activities <ul style="list-style-type: none"> ▪ Acceptable Use Policy updates ▪ Tool/PC Security ▪ Training completed / Required notifications ▪ Non-Disclosure Agreement(s)
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management	1.1.1.1	Access to client consoles and/or pre-determined designed view is to be managed via LDAPS AD Group(s)
Visitor Management	1.1.1.2	All access to views within EOC-DC managed locations are to be pre-determined by the following:
Visitor Management	1.1.1.2.1	<ul style="list-style-type: none"> • Job description for view access • All Access is approved by EOC-DC Management • Active Directory (AD) Group managed
Visitor Management		
Visitor Management		
Visitor Management	2 Data Retention	
Visitor Management	2.1 All reservation data retention is to be defined on a point by point basis as determined by EOC-DC Management for the following	
Visitor Management	2.1.1	Provide reports for selected periods of time for site/personnel/reservation stop-start/authorizer activity

Visitor Management	2.1.2	Must track the following by user either credentialed or not:
Visitor Management		<ul style="list-style-type: none"> Method of Identification provided at start of visit
Visitor Management		<ul style="list-style-type: none"> Devices/Tools
Visitor Management		<ul style="list-style-type: none"> Clock for review (1 yr)
Visitor Management	2.1.3	New or changes to access level is managed through
Visitor Management		<ul style="list-style-type: none"> SOM Automated Form Process via DTMB-0927
Visitor Management		or
Visitor Management		<ul style="list-style-type: none"> Provided a bulk data update method for initial loading/mass updates
Visitor Management	2.1.4	The ability to attach documents to either
Visitor Management		<ul style="list-style-type: none"> User
Visitor Management		<ul style="list-style-type: none"> Reservation
Visitor Management	2.1.5	Track Previous user activity
Visitor Management	2.1.6	Track equipment movement
Visitor Management	2.1.7	Deny or restrict access
Visitor Management	3.0 Issue Management	
Visitor Management	3.1 Visit History retrieval	
Visitor Management	3.1.1 Human Resources Requested	
Visitor Management	3.1.1.1	Follow all associated policies, standards and procedures
Visitor Management	3.1.2 EOC-DC Business process management requested	
Visitor Management	3.1.2.1	Management of reports shall be at the discretion of EOC-DC Facility management or their designee
Visitor Management	4.0 External system integrations	
Visitor Management	4.1	External integrations are to be managed by EOC-DC management and corresponding MOU's with data connections that are application specific

Visitor Management	5.0 Reporting	
Visitor Management	5.1 Formatting	
Visitor Management	5.1.1 All reports are to be generated showing the following information	<ul style="list-style-type: none"> • Time/Date stamped • Who accessed including attempts to access • Devices impacted by previous bullet • Previous/Current value if settings were changed for changes • Location requested
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management	5.2 Frequency of Report Delivery	
Visitor Management	5.2.1 Monthly	First calendar day the Month
Visitor Management	5.2.2 Quarterly	Summary of current month including the previous 2 months
Visitor Management	5.2.3 Annually	Summary of the 4 quarter reports
Visitor Management	5.2.4 Exclusions	HR Request
Visitor Management	6.0 Data retrieval	
Visitor Management	6.1 EOC-DC View/Export	
Visitor Management	6.1.1	EOC-DC reserves the right to view/retrieve on demand reports
Visitor Management	6.1.2	Capability of 24/7/365 availability for onsite staff to maintain situational monitoring
Visitor Management	7.0 SSP Information	
Visitor Management	7.1 Common Control	Must provide all common controls for inclusion into Risk Assessment
Visitor Management	0.0 Data Capture	
Visitor Management	1.0 Reservation Requestor	<p>The purpose of this section is to outline the on-screen data that is required for capture that the Reservation Requestor must provide at the time of reservation submittal.</p> <p>The Reservation Requestor has a screen that details the following:</p> <ul style="list-style-type: none"> • Time and date of reservation
Visitor Management		
Visitor Management		
Visitor Management		

Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management	2.0 Reservation Requestor Management	<ul style="list-style-type: none"> ○ Needs to be able to span multiple days without multiple reservations <ul style="list-style-type: none"> ● Single location per reservation ● End destination at the location ○ Selection should be tied to approved permissions documentation <ul style="list-style-type: none"> ● Authorizing ticket look up ○ RFC ○ Remedy <ul style="list-style-type: none"> ● Reason/Purpose of visit ● Provide list of past/current/future reservations where the user appears as either primary or as attend <ul style="list-style-type: none"> ● List/add to of equipment in possession by name/Serial Number ○ Pre-approved <ul style="list-style-type: none"> ▪ as having been through the entry process before ▪ Only appears if replicated in user profile ○ Current equipment being carried into facility ○ Equipment entering/leaving <ul style="list-style-type: none"> ● Once Reservation Activator adds an ad hoc attendee, they appear with the minimum status (escort only) ○ Any assets assigned to this ad hoc attendee class to be tracked to the attendee ● Alarming of required documentation notification
Visitor Management		
Visitor Management		Per the Access request form (DTMB-0927) the application must provide the following:

Visitor Management		Able to make updates by either bulk or GUI data entry of reservation requestors or materials to be provided
Visitor Management	3.0 Reservation Approver	The purpose of this section is to describe the process and requirements of the Reservation Approver
Visitor Management		<ul style="list-style-type: none"> • Automated Approval <ul style="list-style-type: none"> ○ List of pre-approved personnel whose reservations approval is automated ○ Exceptions <ul style="list-style-type: none"> ▪ Added Ad hoc attendees • Reservation is provided with indicators for approval/denial: <ul style="list-style-type: none"> ○ Green checks next to key components <ul style="list-style-type: none"> ▪ Valid RFC/Remedy ▪ Timeline in RFC matches visit times
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management		
Visitor Management	4.0 Reservation Activator	The purpose of this section is to describe the data the required by the Reservation Activator and scripting for automation
Visitor Management	1.1 Personal Computer (PC) Operating System (OS) level	Windows 10 or higher is recommended
Visitor Management	1.2 Browser Type	Microsoft Edge / Chrome / Firefox or above is recommended as the web portal
Visitor Management	1.3 Connection Type	Users must have an internet browser to use the system
Visitor Management	3 Security Posture	
Visitor Management	3.1 Access controls	
Visitor Management	3.1.1	All data access is to be managed by non-self-signed SSL Certificate with ID/PW
Visitor Management	3.2 Management application user access	
Visitor Management	3.2.1 Group Management	
Visitor Management	3.2.1.1	All access levels are to be managed by LDAPS AD groups and follow the DTMB-0161 and DTMB-927 access process

Visitor Management	3.2.1.2 Levels of access by LDAPS Group (EOC-DC_DVM_<Group Name>)	
Visitor Management	3.2.1.2.1	EOC-DC have the ability to manage the lesser pre-defined roles as follows:
Visitor Management		Has the ability to manipulate pre-defined views available to the Power User and Read Only roles.
Visitor Management		Power User:
Visitor Management		Has the ability to manipulate pan tilt zoom (PTZ) devices with stop and start recording
Visitor Management		Read Only_<Location>:
Visitor Management		Access to view only pre-defined views as designated by ID and location
Visitor Management		Security Vulnerabilities must be remediated by the vendor in a timely manner as part of the Contract
Visitor Management	4 Technology Management	Software updates to new version levels costing must be included as part of the Contract and included in final application management costing
Visitor Management		Planned software updates and patches of application and modules must follow State of Michigan RFC process with EOC-DC being an impacted party

SCHEDULE B – PRICING

The pricing below includes all costs for the licensing, support, implementation, and training for the Solution. This is all inclusive pricing.

Postproduction Warranty. The Contractor must provide a 90 calendar days postproduction warranty at no cost to the State. The postproduction warranty will meet all requirements of the contract, including all Support Services identified in Schedule D.

Travel and Expenses

The State does not pay for overtime or travel expenses.

Total Pricing Summary for all EOC-DC Tools including First Year Support				
Part #	Qty	Description	Unit Price	Ext. Price
VM Visitor Management	1	Combined Quote JEM 24497 for Visitor Management (EntryPoint) & Digital Video Management (Milestone) . Both areas integrating into Lenel. Contractor will write an API for the Nlyte.	\$1,027,000.00	\$1,027,000.00
AC_PA Asset Control and Physical Audit	1	Asset Control and Physical Audit (RFCode)& Nlyte Asset Tagging for LSHC, LMHC & 2 Storage Rooms Readers for Depot, 2 Hannah Storage Rooms & Guard Station Contractor will integrate RFCode with Nlyte Total Assets = 2287 JEM Quote: 24488	\$382,025.00	\$382,025.00
EM Environmental Monitoring	1	Environmental Monitoring for LSHC: RLE & Nlyte Wireless Temperature and Humidity Sensors (Every 3rd cabinet will have 3 temperature sensors on the front door, 3 on the rear door and 1 humidity sensor per aisle.) 10 Smoke Detection throughout Data Center 17 Wireless Leak Detection around the CRACS JEM Quote 24495	\$139,720.00	\$139,720.00
RL Rack Locking	1	Rack Locking for LSHC Two-Factor Authentication Options (Card Swipe and Pin Code) - Integrating into Carrier's Lenel Software JEM Quote 24489	\$851,572.50	\$851,572.50
			Subtotal	\$2,400,317.50
			Tax	\$0.00
			Shipping	\$0.00
			Total	\$2,400,317.50

Total Pricing Summary of Annual Maintenance FY25-28 (FY 24 Maintenance costs are included in the Total Pricing Summary)				
Part #	Qty	Description		Annual Price
SUPPORT VM and DVM	1	D/A Central support and software maintenance. Support is both remote and onsite.		\$73,400.00
RFCODE_LICE AC_PA	1	CenterScape Term Asset: Licensed per Asset (2287) per Year		\$34,875.00
NLYTE_SUPP AC_PA	1	Annual Nlyte Connector Support for RFCODE *		\$12,750.00
SUPPORT EM	1	12-Month Support for Nlyte (RLE's Environmental Monitoring) *		\$2,332.50
dbINF-SR RL	1	db Infinity Maintenance Service for rack handles		\$24,500.00
			Subtotal	147,857.50
			Tax	\$0.00
			Shipping	\$0.00
			Total (Support Fee)	147,857.50

* Annual Increase is limited to the CPI for All Urban Consumers: All items calculated Jan -Jan or 10% whichever is lower

Pricing Breakdown for Visitor Management and Digital Video Management (DVM)				
Part #	Qty	Description	Unit Price	Ext. Price
Service	1	The Lenel OnGuard Security Management and Integration Platform provides integration between the Nlyte, visitor management, video surveillance, and the rack locking systems. This platform will be installed on state provided virtual machines as identified in our proposal. Moving 2 Access control doors to the Lenel system.	\$320,500.00	\$320,500.00
DVM	1	The Video Surveillance System including a video management server and 2 network video recorders, and eighty-four (84) surveillance cameras including 5 years of Milestone Care Plus. Recording will be aggregated at the Lake Superior Hosting	\$379,500.00	\$379,500.00

		Center with redundancy (backup server) installed at Lake Michigan Hosting Center		
VM	1	Visitor Management System including two (2) kiosk workstations to be installed at LSHC and LMHC	\$239,500.00	\$239,500.00
T_D	1	Training and Documentation	\$87,500.00	\$87,500.00
			Subtotal	\$1,027,000.00
			Tax	\$0.00
			Shipping	\$0.00
			Total	\$1,027,000.00

Pricing Breakdown for Asset Control and Physical Audit (RFCode)& Nlyte Asset Tagging				
Part #	Qty	Description	Unit Price	Ext. Price
RFCODE_LIC NSE	1	CenterScape Term Asset: Licensed per Asset (2287) per Year	\$34,875.00	\$34,875.00
RFCODE_ASSE T_TAG	1	RF Code One Time Fee To Include: (25) M250 433 MHz Reader Kit (216) Rack Locator Kit for 40U Racks (70-in) (216) A740 Rack Locator Controller Unit (216) A740 Power Supply (432) Rack Locator LED Strip with blue indicators, 70" for 40U racks (9) Rack Locator Kit for 44U Racks (77-in) (9) A740 Rack Locator Controller Unit (9) A740 Power Supply (18) Rack Locator LED Strip with blue indicators, 77" for 44U racks (18) Rack Locator Kit for 47U Racks (82.25-in) (18) A740 Rack Locator Controller Unit (18) A740 Power Supply (36) Rack Locator LED Stp w blue indicators, 82.25" for 47U racks (243) A740 Extension Cable (60 inch) M/F 3.5mm (243) A740 Signal Splitter (2287) IR-Enabled IT Asset Sensor Only (2400) Flag Tab (4 inch) (200) Thumb Screw Tab (200) Thin Loop Tab (Feed-Thru) (10) Tab Install Keys for M174 IT Asset Loc Sensor (5 Keys) (216) Rack Locator LED Strip with blue indicators,70" for 40U racks	\$154,500.00	\$154,500.00
NLYTE_SOFT	560	Nlyte Connector to RFCode Asset Manager	\$115.00	\$64,400.00
NLYTE_SUPP	1	Annual Nlyte Connector Support (5 X 8)	\$12,750.00	\$12,750.00
RFCODE_SERV ICE	1	Turnkey Installation Services with JEM for Asset Tagging 1) 2 JEM Installers to Install all Readers, Strips, Asset Tags and anything else as part of the BOM 2) RFCode software installation, configuration and installation 3) Includes Nlyte installation of connector	\$115,500.00	\$115,500.00
			Subtotal	\$382,025.00
			Tax	\$0.00
			Shipping	\$0.00
			Total	\$382,025.00

Pricing Breakdown for Environmental Monitoring for LSHC (RLE & Nlyte)

Part #	Qty	Description	Unit Price	Ext. Price
NEO_OPT	311	Nlyte Energy Optimizer	\$37.50	\$11,662.50
SUPPORT	1	12-Month Standard (5x8) Support for Nlyte	\$2,332.50	\$2,332.50
WiNG-MGR	3	WiNG Manager - 900MHz receiver; includes rack mount bracket, PSWA-DC-24 power supply and type A blade	\$2,225.00	\$6,675.00
WiNG-RXT	1	WiNG Range Extender, 900 MHz signals, includes PSWA-DC-5 power supply and type A blade	\$1,827.00	\$1,827.00
WiNG-TH	102	WiNG Temperature/Humidity sensor; 900 MHz wireless transmitter	\$240.50	\$24,531.00
WiNG-LD-LC	17	WiNG Leak Detector; 900 MHz wireless transmitter, includes LC-KIT, requires SC, SC-R, SC-ZH or SD-Z	\$360.00	\$6,120.00
SC-50	17	SeaHawk Sensing Cable; conductive fluids, 50ft (15.24m), pre-installed male/female connectors	\$400.00	\$6,800.00
JC-10	17	J-Clips; qty 10 (for use with SC, SC-R, SC-ZH and NSC)	\$16.00	\$272.00
SERVICE	1	<p>Turnkey Installation of Environmental Monitoring with JEM & Nlyte</p> <p>1) Mount Temperature/Humidity Sensors, where applicable. JEM will work with State for the layout.</p> <p>3) Wireless Leak Detection around the 17 CRACs</p> <p>4) Set up all sensors to be ready to tie into Nlyte Software</p> <p>5) Nlyte Professional Services to be completed</p> <p>***Door Contact Closure is part of the rack locking quote.***</p> <p>Nlyte's Details for all Remote Installation</p> <p>1) DCIM Consultant Sensor Data Load (NAO + NEO) (Remote)</p> <p>2) Configuration for Monitoring and Alarming up to 311 points. Sensors to be added to NAO and Synchronized to NEO Up to 2 new room plans can be added if required</p> <p>3) Project Manager Project Plan and Controls (Remote)</p> <p>For Nlyte only: No Onsite Installation. JEM will be onsite and did include Nlyte onsite assistance, if needed.</p>	\$79,500.00	\$79,500.00
			Subtotal	\$139,720.00
			Tax	\$0.00
			Shipping	\$0.00
			Total	\$139,720.00

**Pricing Breakdown for Rack Locking for LSHC
 Two-Factor Authentication (Pin Code & Card
 Swipe) Integrating into Carrier's Lenel Software**

Part #	Qty	Description	Unit Price	Ext. Price
dbSENTRY-KH KH(S)	240	Cabinet Sentry w/2 Dual Lock Swing Handles (S), 2 Door Contacts, 1 CAT5e Cable 14', Cable Tie Downs, db Sentry Cabinet, and RFID Swing Handle Cabinets are APC & CPI	\$1,920.00	\$460,800.00
dbSENTRY-KH(S)	2	Cabinet Sentry w/ 1 CodeLock-HF Swing Handle (S), 1 Door Contact, 1 CAT5e Cable 14', Cable Tie Downs, db Sentry Cabinet, and RFID Swing Handle APC wall mounted Cabinets	\$1,260.00	\$2,520.00
dbSentry-KRKR -R4R4	49	Cabinet Sentry w/2 Dual Readers & 2 R4 Latch Kits, 2 Door Contacts, 1 CAT 5e Cable Tie Downs for 21 Floor PDUs, 12 EMC and 7 Teradata Cabinets	\$2,075.00	\$101,675.00
db Power	291	Auxiliary Power Supply for db Sentry 110V or 208V	\$57.50	\$16,732.50
dbDC10	240	Surface Mount Door Contacts no resistors and no wires, (only needed if there are split rear doors)	\$39.00	\$9,360.00
dbDC1W	122	Door Contacts (10K) with wires Side panel contacts. Assumes 1 panel per side	\$43.50	\$5,307.00
dbLOGI-500	1	DAS server/client package & LENEL OnGuard Integration Software for connection up to 500 units	\$29,500.00	\$29,500.00
OK5427 V2	1	Omnikey 5427 V2 Multi-class Card Reader/Writer	\$225.00	\$225.00
dbDASSQL-CR W	9	DAS Server/Client package including a card reader/writer	\$717.00	\$6,453.00
dbINF-SR	1	db Infinity Maintenance Service - from Shipment of Handles to LSHC	\$24,500.00	\$24,500.00
INSTALL	1	JEM Turnkey Installation & Training for 291 Cabinets in LSHC 1) Remove old handles 2) Install new front and rear door handles, door and side panel contacts including all the wiring 3) JEM will supply materials to neatly organize all the wiring for the handles and contacts 4) Installation of Software and integration into Lenel 5) Training on Handles and Software State will have standard network switches in each cabinet along with an ethernet drop and a valid IP address for the State's network. State is responsible to have 110V or 208V outlet in the rack to power the handles. This installation is using JEM Installers and Digitus directly for software installation and integration into Lenel.	\$194,500.00	\$194,500.00
			Subtotal	\$851,572.50
			Tax	\$0.00
			Shipping	\$0.00
			Total	\$851,572.50

<u>Task Description</u>	<u>Payment</u>
Meetings and Walk throughs to verify all BOMs for all Areas of RFP (DVM, VM, Rack Locking, Asset Tagging and Environmental Monitoring)	N/A
Provide the State all Server Requirements for Lenel, Milestone, EntryPoint, Digitus, rfCode & Nlyte	N/A
Final verification on BOM & order all hardware and software for all areas of RFP (DVM, VM, Rack Locking, Asset Tagging and Environmental Monitoring)	N/A
Hardware & Software: Place all orders (Will Follow Lead Times for all the Manufacturers)	N/A
D/A Central: Digital Video Management System, Visitor Management System, Lenel Access Management System and Nlyte	
Confirm requirements for DVM recording and order Servers	N/A
Deliver DVM Servers to SOM for testing and install. Contractor will invoice after State Acceptance of DVM Servers.	\$90,848.50
Design Approval Completion and Cameras Hardware Arrival. Contractor will invoice after State Acceptance of Camera Hardware.	\$100,542.30
Lenel software installed, preliminary setup completed, cameras delivered to site and installation in process. Contractor will invoice after State Acceptance of Lenel software installation and cameras are delivered.	\$288,618.55
Digital Video Management system (DVMS) server installed, Network Video Recorder (NVR) installed and operational, work begins on training manuals and system documentation. Contractor will invoice after State Acceptance of DVMS and NVR installation.	\$157,747.50

Preliminary Lenel / Nlyte integration, Camera installation and analytics setup continues, Visitor Management server software and setup of workstations, continue work on training manuals and system documentation. Contractor will invoice after State Acceptance of preliminary Lenel/Nlyte integration and setup of VMS software and workstations.	\$159,125.00
Lenel / Nlyte integration continues with rack locking online and passing data to Nlyte, integration with digital video management system complete, operator training for visitor management system complete and transition to new visitor management system complete. Contractor will invoice after State Acceptance of completion of visitor management system.	\$116,068.15
Training complete.	\$5,700.00
Finalize system verification testing, finalize rest of the documentation. Contractor will invoice after State Acceptance. 90-day Postproduction Warranty to begin after State's Acceptance.	\$57,000.00
After the Postproduction Warranty period ends, the State will approve invoice once open issues are closed, if any.	\$51,350.00
<u>Total Including 1st Year's Maintenance*</u>	<u>\$1,027,000.00</u>
RFCode Asset Tagging & Nlyte	
RFCode Software Installation. Contractor will invoice after State Acceptance of RFCode Software.	\$33,131.25
RFCode Hardware Arrival. Contractor will invoice after State Acceptance of RFCode Hardware.	\$146,775.00
Installation of RFCode in Lansing and Grand Rapids. Contractor will invoice after State Acceptance of RFCode Installation at LMHC and LSHC.	\$62,225.00
RFCode Nlyte Integration Software. Contractor will invoice after State Acceptance of RFCode Nlyte Software Integration.	\$73,292.50

RFCode/Nlyte Installation. Contractor will invoice after State Acceptance of RFCode/Nlyte Installation.	\$46,075.00
Training Complete.	\$475.00
Finalize system verification testing, finalize documentation. Contractor will invoice after State Acceptance. 90-day Postproduction Warranty period to begin after State's Acceptance.	\$950.00
After the Postproduction Warranty period ends, the State will approve invoice once open issues are closed, if any.	\$19,101.25
<u>Total Including 1st Year's Maintenance*</u>	<u>\$382,025.00</u>
Rack Locking	
Lenel OnGuard Software for Integration. Contractor will invoice after State Acceptance of Lenel OnGuard Software.	\$28,025.00
Rack Locking Hardware Onsite. Contractor will make partial delivery and will invoice for the amount delivered after State Acceptance of partial delivery of Rack Locking Hardware.	**Amount based on partial delivery
Installation of all the Rack Locking Hardware delivered.	\$37,525.00
Remaining Rack Locking Hardware delivered & Installation Continuation. Contractor will invoice after State Acceptance of final Rack Locking Hardware and installation.	Contractor will invoice remaining balance based on \$600,944.35 minus previous partial delivery payment**
Rack Locking Completion for Hardware Installation and Software Integration. Contractor will invoice after State Acceptance of Rack Locking Hardware Installation and Software Integration complete.	\$63,645.25
Rack locking system Lenel integration, programming, and system verification. Contractor will invoice after State Acceptance of Rack Locking Lenel integration, programming, and system verification complete.	\$68,875.00

Training Complete.	\$4,750.00
Finalize system verification testing, finalize documentation. Contractor will invoice after State Acceptance. 90-day Postproduction Warranty to begin after State's Acceptance.	\$5,229.28
After the Postproduction Warranty period ends, the State will approve invoice once open issues are closed, if any.	\$42,578.62
<u>Total Including 1st Year's Maintenance*</u>	<u>\$851,572.50</u>
Environmental Monitoring	
Nlyte Software for Environmental Monitoring. Contractor will invoice after State Acceptance of Nlyte Software for Environmental Monitoring.	\$11,079.38
Environmental Monitoring Hardware Arrives. Contractor will invoice after State Acceptance of Environmental Monitoring Hardware.	\$46,129.62
Environmental Monitoring Installation (This could be done sooner, after rack locking and asset tagging is completed.) Contractor will invoice after State Acceptance of Environmental Monitoring Installation.	\$23,275.00
Environmental Monitoring Integration into Nlyte Completion. Contractor will invoice after State Acceptance of Environmental Monitoring Integration into Nlyte Completion.. 90-day Postproduction Warranty to begin after State's Acceptance.	\$52,250.00
After the Postproduction Warranty period ends, the State will approve invoice once open issues are closed, if any.	\$6,986.00
<u>Total Including 1st Year's Maintenance*</u>	<u>\$139,720.00</u>
Total of All Areas	\$2,400,317.50

*** Annual Maintenance period after the 1st Year for each category (VM, AC PA, EM, and RL) will begin 12 months after the respective 90-Day Postproduction Warranty period for each category type. This will result in maintenance renewals occurring on varying dates. However,**

the State will have the ability to co-term all the license maintenance costs at its discretion in the future.

SCHEDULE C - INSURANCE SCHEDULE

Required Coverage.

1.1 **Insurance Requirements.** Contractor, at its sole expense, must maintain the insurance coverage identified below. All required insurance must: (i) protect the State from claims that arise out of, are alleged to arise out of, or otherwise result from Contractor's or subcontractor's performance; (ii) be primary and non-contributing to any comparable liability insurance (including self-insurance) carried by the State; and (iii) be provided by a company with an A.M. Best rating of "A-" or better, and a financial size of VII or better.

Required Limits	Additional Requirements
Commercial General Liability Insurance	
<u>Minimal Limits:</u> \$1,000,000 Each Occurrence \$1,000,000 Personal & Advertising Injury \$2,000,000 Products/Completed Operations \$2,000,000 General Aggregate Limit	Policy must be endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds using endorsement CG 20 10 11 85, or both CG 20 10 12 19 and CG 20 37 12 19.
Automobile Liability Insurance	
<u>Minimal Limits:</u> \$1,000,000 Per Accident	Policy must: (1) be endorsed to add "the State of Michigan, its departments, divisions, agencies, offices, commissions, officers, employees, and agents" as additional insureds; and (2) include Hired and Non-Owned Automobile coverage.
Workers' Compensation Insurance	
<u>Minimal Limits:</u> Coverage according to applicable laws governing work activities.	Waiver of subrogation, except where waiver is prohibited by law.
Employers Liability Insurance	
<u>Minimal Limits:</u> \$500,000 Each Accident \$500,000 Each Employee by Disease \$500,000 Aggregate Disease.	
Crime (Fidelity) Insurance	
<u>Minimal Limits:</u> \$1,000,000 Employee Theft Per Loss	Policy must: (1) cover forgery and alteration, theft of money and securities, robbery and safe burglary, computer fraud, funds transfer fraud, money order and counterfeit currency, and (2) be endorsed to add "the State of Michigan, its departments, divisions,

Required Limits	Additional Requirements
	agencies, offices, commissions, officers, employees, and agents” as Loss Payees.

1.2 If any required policies provide claims-made coverage, the Contractor must: (i) provide coverage with a retroactive date before the Effective Date of the Contract or the beginning of Contract Activities; (ii) maintain coverage and provide evidence of coverage for at least three (3) years after completion of the Contract Activities; and (iii) if coverage is cancelled or not renewed, and not replaced with another claims-made policy form with a retroactive date prior to the Effective Date of this Contract, Contractor must purchase extended reporting coverage for a minimum of three (3) years after completion of work.

1.3 Contractor must: (i) provide insurance certificates to the Contract Administrator, containing the agreement or delivery order number, at Contract formation and within twenty (20) calendar days of the expiration date of the applicable policies; (ii) require that subcontractors maintain the required insurances contained in this Section; (iii) notify the Contract Administrator within five (5) business days if any policy is cancelled; and (iv) waive all rights against the State for damages covered by insurance. Failure to maintain the required insurance does not limit this waiver.

1.4 This Section is not intended to and is not to be construed in any manner as waiving, restricting or limiting the liability of either party for any obligations under this Contract (including any provisions hereof requiring Contractor to indemnify, defend and hold harmless the State).

SCHEDULE D - SERVICE LEVEL AGREEMENT

The parties agree as follows:

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this Schedule shall have the respective meanings given to them in the Contract Terms and Conditions.

“Contact List” means a current list of Contractor contacts and telephone numbers set forth in the attached **Schedule D – Attachment 1** to this Schedule to enable the State to escalate its Support Requests, including: (a) the first person to contact; and (b) the persons in successively more qualified or experienced positions to provide the support sought.

“Critical Service Error” has the meaning set forth in the Service Level Table.

“Error” means, generally, any failure or error referred to in the Service Level Table.

“First Line Support” means the identification, diagnosis and correction of Errors by the State.

“High Service Error” has the meaning set forth in the Service Level Table.

“Low Service Error” has the meaning set forth in the Service Level Table.

“Medium Service Error” has the meaning set forth in the Service Level Table.

“Resolve” and the correlative terms, **“Resolved”**, **“Resolving”** and **“Resolution”** each have the meaning set forth in **Section 2.4**

“Service Credit” has the meaning set forth in **Section 3.1**

“Second Line Support” means the identification, diagnosis and correction of Errors by the provision of (a) telephone and email assistance by a qualified individual on the Contact List and remote application support, or (b) on-site technical support at the State's premises by a qualified individual on the Contact List.

“Service Levels” means the defined Error and corresponding required service level responses, response times, Resolutions and Resolution times referred to in the Service Level Table.

“Service Level Table” means the table set out in **Section 2.4**

“State Cause” means any of the following causes of an Error: (a) a State server hardware problem; (b) a desktop/laptop hardware problem; or (c) a State network communication problem.

“State Systems” means the State's information technology infrastructure, including the State's computers, software, databases, electronic systems (including database management systems) and networks.

“Support Hours” means Support hours from 8 a.m. to 5 p.m. EST.

“**Support Request**” has the meaning set forth in **Section 2.2**.

2. Support Services. The State will provide First Line Support prior to making a Service Request for Second Line Support. Contractor shall perform all Second Line Support and other Support Services during the Support Hours throughout the Term in accordance with the terms and conditions of this Schedule and the Contract, including the Service Levels and other Contractor obligations set forth in this **Section 2**.

2.1 Support Service Responsibilities. Contractor shall:

- (a) provide unlimited telephone support during all Support Hours;
- (b) respond to and Resolve all Support Requests in accordance with the Service Levels;
- (c) provide unlimited remote Second Line Support to the State during all Support Hours;
- (d) provide on-premise Second Line Support to the State if remote Second Line Support will not Resolve the Error; and
- (e) provide to the State all such other services as may be necessary or useful to correct an Error or otherwise fulfill the Service Level requirements, including defect repair, programming corrections and remedial programming.

2.2 Support Requests. Once the State has determined that an Error is not the result of a **State Cause**, the State may request Support Services by way of a Support Request. The State shall classify its requests for Error corrections in accordance with the support request classification and definitions of the Service Level Table set forth in **Section 2.4** (each a “**Support Request**”). The State shall notify Contractor of each Support Request by e-mail or telephone. The State shall include in each Support Request a description of the reported Error and the time the State first observed the Error.

2.3 State Obligations. The State shall provide the Contractor with each of the following to the extent reasonably necessary to assist Contractor to reproduce operating conditions similar to those present when the State detected the relevant Error and to respond to and Resolve the relevant Support Request:

- (i) if not prohibited by the State’s security policies, remote access to the State Systems, and if prohibited, direct access at the State’s premises;
- (ii) output and other data, documents and information, each of which is deemed the State’s Confidential Information as defined in the Contract; and
- (iii) such other reasonable cooperation and assistance as Contractor may request.

2.4 Service Level Table. Response and Resolution times will be measured from the time Contractor receives a Support Request until the respective times Contractor has (a) responded to that Support Request, in the case of response time and (b) Resolved that Support Request, in the case of Resolution time. “**Resolve**”, “**Resolved**”, “**Resolution**” and correlative capitalized terms mean, with respect to any particular Support Request, that Contractor has corrected the Error that prompted that Support Request and that the State has confirmed such correction and its acceptance of it in writing. Contractor shall respond to and Resolve all Support Requests within the following times based on the State’s designation of the severity of the associated Error, subject to the parties’ written agreement to revise such designation after Contractor’s investigation of the reported Error and consultation with the State:

Support Request Classification	Definition	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)
Critical Service Error	(a) Issue affecting entire system or single critical production function; (b) Software down or operating in materially degraded state; (c) Data integrity at risk; (d) Material financial impact; (e) Widespread access interruptions: or (f) Classified by the state as a Critical Service Error	Contractor shall acknowledge receipt of a Support Request within thirty (30) minutes.	Contractor shall Resolve the Support Request as soon as practicable and no later than four (4) hours after Contractor's receipt of the Support Request. If the Contractor Resolves the Support Request by way of a work-around accepted in writing by the State, the support classification assessment will be reduced to a High Service Error.
High Service Error	(a) A Critical Service Error for which the State has received, within the Resolution time for Critical Service Errors, a work-around that the State has accepted in writing; or (b) Primary component failure that materially impairs systems performance; (c) Data entry or access is materially impaired on a limited basis; or (d) performance issues of severe nature impacting critical processes	Contractor shall acknowledge receipt of a Support Request or, where applicable, the State's written acceptance of a Critical Service Error work-around, within twenty-four (24) hours.	Contractor shall Resolve the Support Request as soon as practicable and no later than two (2) Business Days after Contractor's receipt of the Support Request or, where applicable, the State's written acceptance of a Critical Service Error work-around.

Support Request Classification	Definition	Service Level Metric (Required Response Time)	Service Level Metric (Required Resolution Time)
Medium Service Error	An isolated or minor Error in the Software that meets any of the following requirements: (a) does not significantly affect Software functionality; (b) can or does impair or disable only certain non-essential Software functions; or (c) does not materially affect the State's use of the Software	Contractor shall acknowledge receipt of the Support Request within two (2) Business Days.	Contractor shall Resolve the Support Request as soon as practicable and no later than ten (10) Business Days after Contractor's receipt of the Support Request.
Low Service Error	Request for assistance, information, or services that are routine in nature.	Contractor shall acknowledge receipt of the Support Request within five (5) Business Days.	N/A

2.5 Escalation. If Contractor does not respond to a Support Request within the relevant Service Level response time, the State may escalate the Support Request to the Contractor Project Manager and State Program Managers, or their designees, and then to the parties' respective Contract Administrators.

2.6 Time Extensions. The State may, on a case-by-case basis, agree in writing to a reasonable extension of the Service Level response or Resolution times.

2.7 Contractor Updates. Contractor shall give the State monthly electronic or other written reports and updates of:

- (a) the nature and status of its efforts to correct any Error, including a description of the Error and the time of Contractor's response and Resolution;
- (b) its Service Level performance, including Service Level response and Resolution times; and
- (c) the Service Credits to which the State has become entitled.

3. Service Credits.

3.1 Service Credit Amounts. If the Contractor fails to respond to a Support Request within the applicable Service Level response time or to Resolve a Support Request within the applicable Service Level Resolution time,

the State will be entitled to the corresponding service credits specified in the table below ("**Service Credits**"), provided that the relevant Error did not result from a State Cause.

Support Request Classification	Service Level Credits (For Failure to Respond to any Support Request Within the Corresponding Response Time)	Service Level Credits (For Failure to Resolve any Support Request Within the Corresponding Required Resolution Time)
Critical Service Error	An amount equal to 5% of the then current monthly Support Fee for each hour by which Contractor's response exceeds the required Response time.	An amount equal to 5% of the then current monthly Support Fee for each hour by which Contractor's Resolution of the Support Request exceeds the required Resolution time.
High Service Error	An amount equal to 3% of the then current monthly Support Fee for each Business Day, and a pro-rated share of such percentage for each part of a Business Day, by which Contractor's response exceeds the required Response time.	An amount equal to 3% of the then current monthly Support Fee for each Business Day, and a pro-rated share of such percentage for each part of a Business Day, by which Contractor's Resolution of the Support Request exceeds the required Resolution time.

3.2 Compensatory Purpose. The parties intend that the Service Credits constitute compensation to the State, and not a penalty. The parties acknowledge and agree that the State's harm caused by Contractor's delayed delivery of the Support Services would be impossible or very difficult to accurately estimate as of the Effective Date, and that the Service Credits are a reasonable estimate of the anticipated or actual harm that might arise from Contractor's breach of its Service Level obligations.

3.3 Issuance of Service Credits. Contractor shall, for each monthly invoice period, issue to the State, together with Contractor's invoice for such period, a written acknowledgment setting forth all Service Credits to which the State has become entitled during that invoice period. Contractor shall pay the amount of the Service Credit as a debt to the State within fifteen (15) Business Days of issue of the Service Credit acknowledgment, provided that, at the State's option, the State may, at any time prior to Contractor's

3.4 of such debt, deduct the Service Credit from the amount payable by the State to Contractor pursuant to such invoice.

3.5 Additional Remedies for Service Level Failures. Contractor's repeated failure to meet the Service Levels for Resolution of any Critical Service Errors or High Service Errors, or any combination of such Errors, within the applicable Resolution time set out in the Service Level Table will constitute a material breach under the Contract. Without limiting the State's right to receive Service Credits under this **Section 4**, the State may terminate this Schedule for cause in accordance with terms of the Contract.

4. Communications. In addition to the mechanisms for giving notice specified in the Contract, unless expressly specified otherwise in this Schedule or the Contract, the parties may use e-mail for communications on any matter referred to herein.

SCHEDULE D - Attachment 1 – Contact List

Jami Moore
23537 Lakepointe Dr
Clinton Twp., MI 48036
j.moore@jemtechgroup.com
586-783-3400

SCHEDULE E – DATA SECURITY REQUIREMENTS

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this **Schedule** shall have the respective meanings given to them in the Contract.

“**Contractor Security Officer**” has the meaning set forth in **Section 2** of this Schedule.

“**FedRAMP**” means the Federal Risk and Authorization Management Program, which is a federally approved risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

“**FISMA**” means The Federal Information Security Modernization Act of 2014 (Pub.L. No. 113-283 (Dec. 18, 2014)).

“**Hosting Provider**” means any Permitted Subcontractor that is providing any or all of the Hosted Services under this Contract.

“**NIST**” means the National Institute of Standards and Technology.

“**PCI**” means the Payment Card Industry.

“**PSP**” or “**PSPs**” means the State’s IT Policies, Standards and Procedures.

“**SSAE**” means Statement on Standards for Attestation Engagements.

“**Security Accreditation Process**” has the meaning set forth in **Section 6** of this Schedule

2. Security Officer. Contractor will appoint a Contractor employee to respond to the State’s inquiries regarding the security of the Hosted Services who has sufficient knowledge of the security of the Hosted Services and the authority to act on behalf of Contractor in matters pertaining thereto (“**Contractor Security Officer**”).

3. Contractor Responsibilities. Contractor is responsible for establishing and maintaining a data privacy and information security program, including physical, technical, administrative, and organizational safeguards, that is designed to:

- (a) ensure the security and confidentiality of the State Data;
- (b) protect against any anticipated threats or hazards to the security or integrity of the State Data;
- (c) protect against unauthorized disclosure, access to, or use of the State Data;
- (d) ensure the proper disposal of any State Data in Contractor’s or its subcontractor’s possession; and
- (e) ensure that all Contractor Representatives comply with the foregoing.

The State has established Information Technology (IT) PSPs to protect IT resources under the authority outlined in the overarching State 1305.00 Enterprise IT Policy. In no case will the safeguards of Contractor’s data privacy and information security program be less stringent than the safeguards used by the State, and Contractor must at all times comply with all applicable public and non-public State IT policies and standards, of which the publicly available ones are at https://www.michigan.gov/dtmb/0,5552,7-358-82547_56579_56755---,00.html.

This responsibility also extends to all service providers and subcontractors with access to State Data or an ability to impact the contracted solution. Contractor responsibilities are determined from the PSPs based on the services being provided to the State, the type of IT solution, and the applicable laws and regulations.

4. Acceptable Use Policy. To the extent that Contractor has access to the State's IT environment, Contractor must comply with the State's Acceptable Use Policy, see https://www.michigan.gov/documents/dtmb/1340.00.01_Acceptable_Use_of_Information_Technology_Standard_458958_7.pdf. All Contractor Personnel will be required, in writing, to agree to the State's Acceptable Use Policy before accessing State systems. The State reserves the right to terminate Contractor's and/or subcontractor(s) or any Contractor Personnel's access to State systems if the State determines a violation has occurred.

5. Protection of State's Information. Throughout the Term and at all times in connection with its actual or required performance of the Services, Contractor will:

5.1 If Hosted Services are provided by a Hosting Provider, ensure each Hosting Provider maintains FedRAMP authorization for all Hosted Services environments throughout the Term, and in the event a Hosting Provider is unable to maintain FedRAMP authorization, the State, at its sole discretion, may either a) require the Contractor to move the Software and State Data to an alternative Hosting Provider selected and approved by the State at Contractor's sole cost and expense without any increase in Fees, or b) immediately terminate this Contract for cause pursuant to **Section 15.1** of the Contract;

5.2 for Hosted Services provided by the Contractor, maintain either a FedRAMP authorization or an annual SSAE 18 SOC 2 Type II audit based on State required NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs.

5.3 ensure that the Software and State Data is securely stored, hosted, supported, administered, accessed, and backed up in the continental United States, and the data center(s) in which the data resides minimally meet Uptime Institute Tier 3 standards (www.uptimeinstitute.com), or its equivalent;

5.4 maintain and enforce an information security program including safety and physical and technical security policies and procedures with respect to its Processing of the State Data that complies with the requirements of the State's data security policies as set forth in this Contract, and must, at a minimum, remain compliant with FISMA and NIST Special Publication 800-53 MOD Controls using identified controls and minimum values as established in applicable State PSPs;

5.5 provide technical and organizational safeguards against accidental, unlawful or unauthorized access to or use, destruction, loss, alteration, disclosure, encryption, transfer, commingling or processing of such information that ensure a level of security appropriate to the risks presented by the processing of State Data and the nature of such State Data, consistent with best industry practice and applicable standards (including, but not limited to, compliance with FISMA, NIST, CMS, IRS, FBI, SSA, HIPAA, FERPA and PCI requirements as applicable);

5.6 take all reasonable measures to:

(a) secure and defend all locations, equipment, systems and other materials and facilities employed in connection with the Services against "malicious actors" and others who may seek, without authorization, to destroy, disrupt, damage, encrypt, modify, copy, access or otherwise use Hosted Services or the information found therein; and

(b) prevent (i) the State and its Authorized Users from having access to the data of other customers or such other customer's users of the Services; (ii) State Data from being commingled with or

contaminated by the data of other customers or their users of the Services; and (iii) unauthorized access to any of the State Data;

5.7 ensure that State Data is encrypted in transit and at rest using FIPS validated AES encryption modules and a key size of 128 bits or higher;

5.8 ensure the Hosted Services support Identity Federation/Single Sign-on (SSO) capabilities using Security Assertion Markup Language (SAML), Open Authentication (OAuth) or comparable State approved mechanisms;

5.9 ensure the Hosted Services implements NIST compliant multi-factor authentication for privileged/administrative and other identified access.

5.10 Throughout the Term, Contractor must not provide Hardware or Services from the list of excluded parties in the System for Award Management (SAM) (<https://www.sam.gov>) for entities excluded from receiving federal government awards for "covered telecommunications equipment or services".

6. Security Accreditation Process. Throughout the Term, Contractor will assist the State, at no additional cost, with its **Security Accreditation Process**, which includes the development, completion and on-going maintenance of a system security plan (SSP) using the State's automated governance, risk and compliance (GRC) platform, which requires Contractor to submit evidence, upon request from the State, in order to validate Contractor's security controls within two weeks of the State's request. On an annual basis, or as otherwise required by the State such as for significant changes, re-assessment of the system's controls will be required to receive and maintain authority to operate (ATO). All identified risks from the SSP will be remediated through a Plan of Action and Milestones (POAM) process with remediation time frames and required evidence based on the risk level of the identified risk. For all findings associated with the Contractor's solution, at no additional cost, Contractor will be required to create or assist with the creation of State approved POAMs, perform related remediation activities, and provide evidence of compliance. The State will make any decisions on acceptable risk, Contractor may request risk acceptance, supported by compensating controls, however only the State may formally accept risk. Failure to comply with this section will be deemed a material breach of the Contract.

7. Unauthorized Access. Contractor may not access, and must not permit any access to, State systems, in whole or in part, whether through the Hosted Services or otherwise, without the State's express prior written authorization. Such authorization may be revoked by the State in writing at any time in its sole discretion. Any access to State systems must be solely in accordance with the Contract and this Schedule, and in no case exceed the scope of the State's authorization pursuant to this Section. All State-authorized connectivity or attempted connectivity to State systems shall be only through the State's security gateways and firewalls and in compliance with the State's security policies set forth in the Contract as the same may be supplemented or amended by the State and provided to Contractor from time to time.

8. Security Audits.

8.1 During the Term, Contractor will maintain complete and accurate records of its data protection practices, IT security controls, and the security logs relating to State Data, including but not limited to any backup, disaster recovery or other policies, practices or procedures relating to the State Data and any other information relevant to its compliance with this Contract.

8.2 Without limiting any other audit rights of the State, the State has the right to review Contractor's data privacy and information security program prior to the commencement of Services and from time to time during the term of this Contract. The State, at its own expense, is entitled to perform, or to have performed, an on-site audit of Contractor's data privacy and information security program. If the State chooses to perform an on-site audit, Contractor will, make all such records, appropriate personnel and relevant materials available

during normal business hours for inspection and audit by the State or an independent data security expert that is reasonably acceptable to Contractor, provided that the State: (i) gives Contractor at least five (5) Business Days prior notice of any such audit; (ii) undertakes such audit no more than once per calendar year, except for good cause shown; and (iii) conducts or causes to be conducted such audit in a manner designed to minimize disruption of Contractor's normal business operations and that complies with the terms and conditions of all data confidentiality, ownership, privacy, security and restricted use provisions of the Contract. The State may, but is not obligated to, perform such security audits, which shall, at the State's option and request, include penetration and security tests, of any and all Hosted Services and their housing facilities and operating environments.

8.3 During the Term, Contractor will, when requested by the State, provide a copy of Contractor's and Hosting Provider's FedRAMP System Security Plan(s) or SOC 2 Type 2 report(s) to the State within two weeks of the State's request. The System Security Plan and SSAE audit reports will be recognized as Contractor's Confidential Information.

8.4 With respect to State Data, Contractor must implement any required safeguards as identified by the State or by any audit of Contractor's data privacy and information security program.

8.5 The State reserves the right, at its sole election, to immediately terminate this Contract or a Statement of Work without limitation and without liability if the State determines that Contractor fails or has failed to meet its obligations under this **Section 8**.

9. Application Scanning. During the Term, Contractor must, at its sole cost and expense, scan all Contractor provided applications, and must analyze, remediate and validate all vulnerabilities identified by the scans as required by the State Secure Web Application and other applicable PSPs.

Contractor's application scanning and remediation must include each of the following types of scans and activities:

9.1 Dynamic Application Security Testing (DAST) – Scanning interactive application for vulnerabilities, analysis, remediation, and validation (may include Interactive Application Security Testing (IAST)).

(a) Contractor must either a) grant the State the right to dynamically scan a deployed version of the Software; or b) in lieu of the State performing the scan, Contractor must dynamically scan a deployed version of the Software using a State approved application scanning tool, and provide the State with a vulnerabilities assessment after Contractor has completed such scan. These scans and assessments i) must be completed and provided to the State quarterly (dates to be provided by the State) and for each major release; and ii) scans must be completed in a non-production environment with verifiable matching source code and supporting infrastructure configurations or the actual production environment.

9.2 Static Application Security Testing (SAST) - Scanning source code for vulnerabilities, analysis, remediation, and validation.

(a) For Contractor provided applications, Contractor, at its sole expense, must provide resources to complete static application source code scanning, including the analysis, remediation and validation of vulnerabilities identified by application source code scans. These scans must be completed for all source code initially, for all updated source code, and for all source code for each major release and Contractor must provide the State with a vulnerability assessment after Contractor has completed the required scans.

9.3 Software Composition Analysis (SCA) – Third Party and/or Open Source Scanning for vulnerabilities, analysis, remediation, and validation.

(a) For Software that includes third party and open source software, all included third party and open source software must be documented and the source supplier must be monitored by the

Contractor for notification of identified vulnerabilities and remediation. SCA scans may be included as part of SAST and DAST scanning or employ the use of an SCA tool to meet the scanning requirements. These scans must be completed for all third party and open source software initially, for all updated third party and open source software, and for all third party and open source software in each major release and Contractor must provide the State with a vulnerability assessment after Contractor has completed the required scans if not provided as part of SAST and/or DAST reporting.

9.4 In addition, application scanning and remediation may include the following types of scans and activities if required by regulatory or industry requirements, data classification or otherwise identified by the State.

(a) If provided as part of the solution, all native mobile application software must meet these scanning requirements including any interaction with an application programming interface (API).

(b) Penetration Testing – Simulated attack on the application and infrastructure to identify security weaknesses.

10. Infrastructure Scanning.

10.1 For Hosted Services, Contractor must ensure the infrastructure and applications are scanned using an approved scanning tool (Qualys, Tenable, or other PCI Approved Vulnerability Scanning Tool) at least monthly and provide the scan's assessments to the State in a format that is specified by the State and used to track the remediation. Contractor will ensure the remediation of issues identified in the scan according to the remediation time requirements documented in the State's PSPs.

11. Nonexclusive Remedy for Security Breach.

11.1 Any failure of the Services to meet the requirements of this Schedule with respect to the security of any State Data or other Confidential Information of the State, including any related backup, disaster recovery or other policies, practices or procedures, is a material breach of the Contract for which the State, at its option, may terminate the Contract immediately upon written notice to Contractor without any notice or cure period, and Contractor must promptly reimburse to the State any Fees prepaid by the State prorated to the date of such termination.

SCHEDULE E, Attachment 1 – Tax Regulation, PCI Compliance, CEPAS, and CJIS, etc....

1. PCI Compliance.

Contractors that process, transmit store or affect the security of credit/debit cardholder data, must adhere to the PCI Data Security Standard. The Contractor is responsible for the security of cardholder data in its possession. The data may only be used to assist the State or for other uses specifically authorized by law.

The Contractor must notify the State's Contract Administrator (within 48 hours of discovery) of any breaches in security where cardholder data has been compromised. In that event, the Contractor must provide full cooperation to the card associations (e.g. Visa, MasterCard, Discover, and American Express) and state acquirer representative(s), or a PCI approved third party, to conduct a thorough security review. The Contractor must provide, at the request of the State, the results of such third party security review. The review must validate compliance with the PCI Data Security Standard for protecting cardholder data. At the State's sole discretion, the State may perform its own security review, either by itself or through a PCI approved third party.

The Contractor is responsible for all costs incurred as the result of the breach. Costs may include, but are not limited to, fines/fees for non-compliance, card reissuance, credit monitoring, and any costs associated with a card association, PCI approved third party, or State initiated security review.

Without limiting Contractor's obligations of indemnification as further described in this Contract, Contractor must indemnify, defend, and hold harmless the State for any and all claims, including reasonable attorneys' fees, costs, and incidental expenses, which may be suffered by, accrued against, charged to, or recoverable from the State in connection with the breach.

The Contractor must dispose of cardholder data when it is no longer needed in compliance with PCI DSS policy. The Contractor must continue to treat cardholder data as confidential upon contract termination.

The Contractor must provide the State's Contract Administrator with an annual Attestation of Compliance (AOC) if or a Report on Compliance (ROC) showing the contractor is in compliance with the PCI Data Security Standard. The Contractor must notify the State's Contract Administrator of all failures to comply with the PCI Data Security Standard.

2. CEPAS Electronic Receipt Processing Standard.

All electronic commerce applications that allow for electronic receipt of credit or debit card and electronic check transactions must be processed via the State's Centralized Electronic Payment Authorization System (CEPAS). To minimize the risk to the State, full credit/debit card numbers, sensitive authentication data, and full bank account information must never be stored on state-owned IT resources. For additional information, refer to the CEPAS Integration Guide that can be found at:

<https://stateofmichigan.sharepoint.com/teams/insidetreasury/about-treasury/work-areas/Documents/CEPAS/Integration%20Guides%20and%20Hotfix%20Notes/PayPoint%20Merchant%20Integration%20Guide%202.14.2021.pdf?CT=1623169629598&OR=Outlook-Body&CID=97F008F1-D094-4ED7-9335-63E0B12988E6>

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE

INFORMATION SERVICES SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A- 130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI1000 Custer Hollow Road
Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE
INFORMATION SERVICES SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee Date

Printed Name/Signature of Contractor Representative Date

Organization and Title of Contractor Representative

Exhibit 7 IRS Publication 1075

Exhibit 7 Safeguarding Contract Language

I. PERFORMANCE

In performance of this contract, the Contractor agrees to comply with and assume responsibility for compliance by officers or employees with the following requirements:

- (1) All work will be performed under the supervision of the contractor.
- (2) The contractor and contractor's officers or employees to be authorized access to FTI must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to FTI. Such list will be provided to the agency and, upon request, to the IRS.
- (3) FTI in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract. FTI in any format shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Inspection or disclosure of FTI to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.
- (4) FTI will be accounted for upon receipt and properly stored before, during, and after processing. In addition, any related output and products require the same level of protection as required for the source material.
- (5) The contractor will certify that FTI processed during the performance of this contract will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of physical and electronic data storage is not possible, the contractor will certify that any FTI in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of FTI will be given to the agency. When this is not possible, the contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.
- (7) All computer systems receiving, processing, storing, or transmitting FTI must meet the requirements in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
- (8) No work involving FTI furnished under this contract will be subcontracted without the prior written approval of the IRS.
- (9) Contractor will ensure that the terms of FTI safeguards described herein are included, without modification, in any approved subcontract for work involving FTI.
- (10) To the extent the terms, provisions, duties, requirements, and obligations of this contract apply to performing services with FTI, the contractor shall assume toward the subcontractor all obligations, duties and responsibilities that the agency under this contract assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties and responsibilities which the contractor assumes toward the agency under this contract.

(11) In addition to the subcontractor's obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and

obligated to the agency under this contract.

(12) For purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses FTI, and the term "subcontractor" includes any officer or employee of the subcontractor with access to or who uses FTI.

(13) The agency will have the right to void the contract if the contractor fails to meet the terms of FTI safeguards described herein.

II. CRIMINAL/CIVIL SANCTIONS

(1) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that FTI disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any FTI for a purpose not authorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution.

(2) Each officer or employee of a contractor to whom FTI is or may be accessible shall be notified in writing that FTI accessible to such officer or employee may be accessed only for a purpose and to the extent authorized herein, and that access/inspection of FTI without an official need-to-know for a purpose not authorized herein constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution.

(3) Each officer or employee of a contractor to whom FTI is or may be disclosed shall be notified in writing that any such unauthorized access, inspection or disclosure of FTI may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of \$1,000 for each unauthorized access, inspection, or disclosure, or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection or disclosure which is the result of gross negligence, punitive damages, plus the cost of the action. These penalties are prescribed by IRC sections 7213, 7213A and 7431 and set forth at 26 CFR 301.6103(n)-1.

(3) Additionally, it is incumbent upon the contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(4) Granting a contractor access to FTI must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding FTI. A contractor and each officer or employee must maintain their authorization to access FTI through annual recertification of their understanding of the agency's security policy and procedures for safeguarding FTI. The initial certification and recertifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC sections 7213, 7213A, and 7431 ([see Exhibit 4, Sanctions for Unauthorized Disclosure](#), and [Exhibit 5, Civil Damages for Unauthorized Disclosure](#)). The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For the initial certification and the annual recertifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the contractor to inspect facilities and operations performing any work with FTI under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process or transmit FTI. Based on the inspection, corrective actions may be required in cases where the contractor is found to be noncompliant with FTI safeguard requirements.

SCHEDULE F – Transition In and Out

Contractor will work with the State to determine the implementation priorities of this entire statement of work for this 5-year agreement. Once the priorities are determined, Contractor will set up the milestones/deliverables timelines for each area included in this Contract. Some of the areas, i.e., asset tagging, and visitor management may be able to implement simultaneously.

Schedule G

Hardware

1. **Definitions.** All initial capitalized terms in this Schedule that are not defined herein shall have the respective meanings given to them in the Contract.
2. **Hardware.** Contractor must provide fully functioning Hardware that fully integrates with the Software.
3. **Delivery.** Contractor must deliver the Hardware to the locations designated by the State by the delivery date specified in the Statement of Work. Five days prior to the actual delivery date, Contractor must give written notice to the State specifying the precise delivery date and time. Contractor must pay all costs associated with replacing any item damaged in transit to the final destination. Contractor acknowledges that no item will be considered delivered on the delivery date if it is damaged or otherwise not ready for the State to begin its acceptance procedures. Contractor must, at a minimum, package the Hardware according to industry standards and include a packing slip with each shipment. Contractor must also arrange for any rigging and drayage necessary to deliver the Hardware. All costs associated with packaging, shipping, transportation, delivery and insurance are to be borne by Contractor.
4. **Installation, Integration and Configuration.**
 - a. Contractor must unpack, assemble, install, integrate, interconnect, configure and otherwise provide and make fully operational all the Hardware at the locations specified in the Statement of Work prior to the applicable Milestone Date in accordance with the criteria set forth in a Statement of Work and the Implementation Plan. Where necessary to complete installation, Contractor must provide all required moving and installation resources, including but not limited to personnel, packing material, and floor protection panels as necessary. After completing installation, Contractor must provide the State with written notification that the Hardware is ready for use.
 - b. Contractor must supply all materials required to complete the assembly, installation, integration, interconnection, and configuration of the Hardware at the locations specified in the Statement of Work so that they are ready for use and acceptance, including providing and setting up all required connections to the power supply and any other necessary cables and any other accessories or supplies.
 - c. Contractor must leave all work areas clean once installation is complete, which includes removing and disposing of all packing materials.
 - d. Unless otherwise provided for in the Pricing Schedule, all costs associated with the installation services described in this Section are to be borne by Contractor.
5. **Documentation.** Contractor must provide to the State all end-user documentation for the Hardware. The documentation, at a minimum, must include all the documentation available to consumers from the manufacturer of the Hardware about the technical specifications of the Hardware, installation requirements, and operating instructions, as well as details about the software programs with which the Hardware functions.
6. **Acceptance.** The section applies generally to the acceptance of Hardware but is subject to the more specific testing and acceptance, if any, in the Statement of Work if the Hardware being tested is part of the testing process involving Software.
 - a. The Hardware is subject to inspection and acceptance by the State. As part of its acceptance process, the State may test any function of the Hardware to determine whether they meet the requirements set forth in the Statement of Work. If the Hardware does not meet the requirements set forth in the Statement of Work, the State may reject the Hardware or require that they be corrected at Contractor's sole cost and expense before accepting them.

- b. Acceptance by the State does not relieve Contractor of its responsibility for defects in the Hardware or other failures to meet the requirements of the Statement of Work or of its support and maintenance obligations.
- c. Unless otherwise specified in the Statement of Work, the procedure for acceptance will be as stated in the Contract for non-Software deliverables.

7. Support and Warranty for Hardware.

- a. Contractor will provide maintenance and support of the Hardware in accordance with the requirements set forth in the Service Level Agreement.
- b. Contractor will provide and assign or otherwise transfer to the State or its designee all manufacturer's warranties regarding all Hardware or as otherwise provided for in the Contract.

8. Hardware Further Representations and Warranties. Contractor represents and warrants that:

- a. all Hardware is delivered free from any security interest, lien, or encumbrance and will continue in that respect; and
- b. the Hardware will not infringe the patent, trademark, copyright, trade secret, or other proprietary rights of any third party.
- c. all hardware includes the manufacturing warranty.

9. Risk of Loss and Title. Until final acceptance, title and risk of loss or damage to Hardware remains with Contractor. Contractor is responsible for filing, processing, and collecting all damage claims. The State will record and report to Contractor any evidence of visible damage. If the State rejects the Hardware, Contractor must remove them from the premises within 10 calendar days after notification of rejection. The risk of loss of rejected or non-conforming Hardware remains with Contractor. Rejected Hardware not removed by Contractor within 10 calendar days will be deemed abandoned by Contractor, and the State will have the right to dispose of it as its own property. Contractor must reimburse the State for costs and expenses incurred in storing or effecting removal or disposition of rejected Hardware. Title passes to the State upon final acceptance of the Hardware.

SCHEDULE H

USER ACCEPTANCE TESTING

The parties agree as follows:

1. Definitions. For purposes of this Schedule, the following terms have the meanings set forth below. All initial capitalized terms in this Schedule that are not defined in this Section 1 have the respective meanings given to them in the Contract.

“**Acceptance**” has the meaning set forth in Section 3.5 of this Schedule.

“**Acceptance Tests**” means such tests as may be conducted in accordance with Section 3 of this Schedule and the Statement of Work to determine whether the Software meets the Requirements.

“**Defect**” means any failure or failures of the Software or Hardware to conform to the Requirements, and any applicable specifications set forth in the Documentation.

“**Integration Testing**” has the meaning set forth in Section 3.1(c) of this Schedule.

“**SUITE**” means the State Unified Information Technology Environment, which was designed and implemented to standardize methodologies, processes, procedures, training, and tools for project management and systems development lifecycle management.

“**Test Data**” means Contractor’s or the State’s test data and testing scripts for use in Acceptance Testing during UAT.

“**Test Environment**” means the operating environment created by Contractor for purposes of UAT.

“**Testing Period**” has the meaning set forth in Section 3.1(b) of this Schedule.

“**Test Results**” means the results Contractor or the State expects to be achieved by processing the Test Data using the Software.

“**UAT**” means User Acceptance Testing.

“**UAT Plan**” means Contractor’s written plan outlining the UAT schedule, procedures for logging Defects and tracking corrections and re-testing status.

2. Parties Obligations for UAT.

2.1 Contractor Obligations. Contractor will complete the following tasks as part of UAT:

- (a) Install, configure and deploy the Software into the Test Environment;
- (b) Install, configure and deploy all related Hardware necessary for the Software to fully function in accordance with the Requirements;
- (c) Create and provide to the State sufficient Test Data and Test Results to adequately test the Software, including testing of any Hardware for purposes of Integration Testing; Vulnerability Tests (Currently using Tenable).
- (d) Review any State-created Test Data and provide necessary feedback to the State;
- (e) Assist the State with completing any necessary SUITE documentation;

- (f) Communicate to the State that the Testing Environment is ready for use prior to initiation of Acceptance Tests;
- (g) Create a written UAT Plan;
- (h) Train State staff on how to perform Acceptance Tests using the UAT Plan. Application administration & usability.
- (i) Correct Defects in Test Results in accordance with Section 3 of this Schedule, which are identified by Contractor or the State during the testing Period;
- (j) Conduct regular status meetings during UAT to assess Test Data and Test Results; and
- (k) Provide a tracking system for Contractor and the State to log Defects and track corrections and re-testing status.

2.2 State Obligations: The State will complete the following tasks as part of UAT:

- (a) Create its own Test Data for use in UAT;
- (b) Develop and add approved tests to the UAT Plan;
- (c) Execute tests and report Test Results to Contractor in accordance with the UAT Plan;
- (d) Participate in regular testing status meetings;
- (e) Enter defects from Test Results into the Contractor-provided issue tracking system. Details to be entered include a minimum of: (i) detailed description of the problem (include screenshot(s) if applicable); and (ii) steps needed to reproduce the issue;
- (f) Perform regular retest of Contractor resolved defects based on mutually agreed schedule; and
- (g) Work with Contractor to prioritize issues that arise during UAT.

3. Acceptance Testing; Acceptance.

3.1 Acceptance Testing.

- (a) Unless otherwise specified in the Statement of Work, upon installation of the Software and Hardware and direction from Contractor that the Software is ready to be tested by the State, acceptance tests will be conducted as set forth in this Section 3 to ensure the Software conforms to the requirements of the Contract, the Statement of Work, and the applicable Requirements.
- (b) All Acceptance Tests will take place at a designated State facility commencing on the Business Day following Contractor's notice that the Software is ready to be tested by the State, and be conducted diligently for up to thirty (30) Business Days, or such other period as may be set forth in the Statement of Work (the "Testing Period"). Acceptance Tests will be conducted by the State, and if requested by the State, Contractor will make suitable Contractor Personnel available to assist or guide such Acceptance Tests. Contractor is solely responsible for all costs and expenses related to Contractor's performance of, participation in, and observation of Acceptance Testing.
- (c) All Hardware must be delivered at the same time as the Software, and Acceptance Tests will also be performed on the integrated system as a whole to ensure full operability, integration, and compatibility among all elements of the Software and Hardware ("Integration Testing").
- (d) The State may suspend Acceptance Tests and the corresponding Testing Period by written notice to Contractor if the State discovers a material Defect in the tested Software or part or feature of the Software. In such

event, Contractor will immediately, and in any case within ten (10) Business Days, correct such Defect, whereupon the Acceptance Tests and Testing Period will resume for the balance of the Testing Period.

3.2 Notices of Completion, Defects, and Acceptance. Within fifteen (15) Business Days following the final completion of all Acceptance Tests, including any Integration Testing, the State will prepare and provide to Contractor written notice of the completion of the tests. Such notice must include a report describing in reasonable detail the tests conducted and the results of such tests, including any uncorrected Defect in the tested Software.

(a) If such notice identifies any Defects, the parties' rights, remedies, and obligations will be as set forth in Section 3.3 and Section 3.4 of this Schedule.

(b) If such notice identifies no Defects, such notice constitutes the State's Acceptance of such Software.

3.3 Failure of Acceptance Tests. If Acceptance Tests identify any Defects, Contractor, at Contractor's sole cost and expense, will remedy all such Defects and re-deliver the Software, in accordance with the Requirements. Re-delivery will occur as promptly as commercially possible and, in any case, within fifteen (15) Business Days following, as applicable, Contractor's receipt of the State's notice under Section 3.2, identifying any Defects.

3.4 Repeated Failure of Acceptance Tests. If Acceptance Tests identify any Defect in the Software after a second or subsequent delivery of the Software, or Contractor fails to re-deliver the Software on a timely basis, the State may, in its sole discretion, by written notice to Contractor:

(a) continue the process set forth in this Section 3; or

(b) deem the failure to be a non-curable material breach of this Contract and the Statement of Work and terminate the Contract for cause.

3.5 Acceptance. Acceptance ("Acceptance") of the Software (subject, where applicable, to the State's right to perform Integration Testing) will occur on the date of the State's delivery of a notice accepting the Software under Section 3.2(b) of this Schedule.

SCHEDULE I – Software License Agreements

List of Software Licenses:

SCHEDULE I, Attachment 1 – NLYTE EULA

SCHEDULE I, Attachment 2 – TECHNOLOGY INDUSTRIES (EntryPoint) EULA

SCHEDULE I, Attachment 3 – RF CODE EULA

SCHEDULE I, Attachment 4 – MILESTONE EULA

SCHEDULE I, Attachment 5 – DIGITUS EULA

SCHEDULE I, Attachment 6 – LENEL EULA

SCHEDULE I, Attachment 1 – NLYTE EULA

AUTOMATED LOGIC CORPORATION DBA NLYTE SOFTWARE
and

STATE OF MICHIGAN DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET

SOFTWARE LICENSE AGREEMENT

AGREED TERMS:	1
1. DEFINITIONS	1
2. LICENSE	1
3. SERVICES.....	2
4. THE CLIENT'S OBLIGATIONS.....	2
5. ACCEPTANCE	3
6. WARRANTIES, ACKNOWLEDGEMENT BY THE CLIENT AND OPPORTUNITY TO FIX	3
7. LIMITATION OF LIABILITY	4
8. CONFIDENTIALITY AND DATA PROTECTION	9
9. INTELLECTUAL PROPERTY RIGHTS	9
10. INDEMNIFICATION.....	6
11. FEES AND PAYMENTS.....	6
12. NON-SOLICITATION	8
13. TERM AND TERMINATION.....	8
14. GENERAL.....	9
SCHEDULE 1 DEFINITIONS.....	11
SCHEDULE 2 MAINTENANCE AND SUPPORT TERMS	14
APPENDIX 1 LICENSED SOFTWARE	17

AGREEMENT dated

2023 ("the Effective Date")

PARTIES:

- (1) **AUTOMATED LOGIC CORPORATION DBA NLYTE SOFTWARE**, a Delaware corporation having a registered office at 1150 Roberts Blvd Kennesaw, Georgia 30144 ("**Licensor**"); and
- (2) **STATE OF MICHIGAN DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET** ("**the Client**" or "**State**").

AGREED TERMS:

6. Definitions. To make this Agreement short and easy to understand, it uses some defined terms which are set forth in Schedule 1 attached hereto.

7. License

- o License Grant. Licensor grants to the Client a perpetual, non-exclusive, non-sublicensable, non-transferable (except as permitted under Section 14.3) license to install and use the Licensed Software up to the Licensed Capacity for the processing of Client's own data and internal governmental purposes subject to the other terms of this Agreement. To the extent that Client engages contractors to host all or any portion of its information technology systems on computers owned or controlled by such contractors, the licenses granted hereunder shall permit the Licensed Software to be installed and operated on such contractors' computer servers provided the Licensed Software is used solely for the purpose of processing Client's governmental data and information and in accordance with the other restrictions set forth in this Agreement.
- o Licensed Capacity. The Licensed Capacity of the Licensed Software is defined in Appendix 1. If Client's use of the Licensed Software exceeds the Licensed Capacity, additional License Fees will be due to purchase the necessary additional Licensed Capacity..These fees will be calculated in accordance with the relevant provisions of Appendix 1. Reseller may invoice the Client for such additional License Fees (and related support fees) pursuant to the terms of the Transaction Document, and the additional License Fees (and related support fees) will be payable to Reseller by Client in accordance with the terms of the Transaction Document. Payment under this provision shall be Licensor's sole and exclusive remedy to cure these issues. If the Client fails to pay to the Reseller such additional License Fees pursuant to the terms of the Transaction Document and if the Client continues to run Licensed Software in excess of the permitted threshold, Licensor may by written notice to the Client and with immediate effect: (a) suspend the Client's license to use the Licensed Software concerned; (b) terminate the license to use the Licensed Software concerned (without terminating this Agreement as a whole); or (c) terminate this Agreement.
- o Further Restrictions on Use. Except as otherwise expressly permitted herein, Client shall not, and shall not permit any third party, to: (i) modify or create any derivative work of any part of the Licensed Software; (ii) rent, lease, or loan the Licensed Software; (iii) permit any third parties (other than its contractors, subcontractors, or other persons authorized by Client) to use the Licensed Software (iv) disassemble, decompile or reverse engineer the Licensed Software or otherwise attempt to gain access to the source code of the Licensed Software or permit the same except as permitted by any applicable law (and to the extent such actions are permitted by applicable law, the Client agrees that before it does so it will make a written request to Licensor for it to supply the relevant information required specifying in reasonable detail the extent and objectives of the proposed decompilation); (v) sell, license, sublicense, publish, distribute, assign or otherwise transfer to a third party the Licensed Software, any copy thereof, or any rights thereto, in whole or in part, except to the extent expressly permitted herein; (vi) copy the Licensed Software except for installing and loading the Licensed Software into computer memory for the purpose of executing the program subject to the Licensed Capacity and except to make a reasonable number of copies solely for back-up and testing purposes; (vii) use the Licensed Software in a service bureau or software as a service capacity (e.g., to process the business data and information of other businesses for their benefit as opposed to for the Client's benefit); (viii) knowingly remove or modify any copyright, trademark, or other proprietary notice of Licensor affixed to the media containing the Licensed Software or appearing within the Licensed Software.
- o Delivery of Software Unless another delivery mechanism is mutually agreed, Licensor shall make the Licensed Software available for download via the Internet through a password protected webpage by the Client promptly after the date hereof. If Client is purchasing Implementation Services (as defined below) pursuant to which Licensor shall be installing the Licensed Software, then at mutually agreed scheduled time Licensor shall on behalf of Client download the Licensed Software and install the Licensed Software on Client's Environment. Upon notifying the Client that the Licensed Software is available for downloading in accordance with this Section 2.4, which notice shall specify the applicable password and login information and Internet address from where the Licensed Software may be downloaded, Licensor shall be deemed to have delivered the Licensed Software for

all purposes hereunder, provided that Licensor continues to make the Licensed Software available for download until the earlier of Client's actual downloading of the Licensed Software or one year after the date hereof.

- Audits. To the extent that a license granted to the Client to use Licensed Software is not unlimited, Licensor may request, either itself or through Reseller, a written certification from the Client regarding use of the Licensed Software for the sole purpose of verifying compliance with this Section 2. Such written certification may occur no more than once in any twelve (12) month period during the term of the Transaction Document. The State will respond to any such request from Licensor within 45 calendar days of receipt. If the Client's use is greater than contracted, such excess use shall be resolved in accordance with Section 2.2 above.

8. Reserved.

9. The Client's Obligations

- Client may provide Licensor with a means to access Licensed Software, but such access will only be permitted with the direct assistance and oversight of a State employee.

10. Reserved..

11. Warranties, acknowledgement by the Client and opportunity to fix

- Software Warranty.

Licensor warrants that for a period of 90 days from delivery of the Licensed Software (the "Warranty Period") the Licensed Software and Documentation provided with those Licensed Software will not contain any Material Errors.

The sole remedy for a breach of the warranty in this Section 6.1 shall be for Licensor to repair or replace the Licensed Software or, if Licensor is unable to do so, refund the License Fee paid for such non-conforming Licensed Software.

- Authority. Each party warrants that it has the right to enter into this Agreement and to grant to the other the rights and licenses granted herein.
- Viruses. Licensor warrants that it shall use commercially reasonable efforts to ensure that the Licensed Software will be free from viruses or other harmful code upon delivery, including but not limited to virus scanning (using an industry-standard and up-to-date virus scanning tool or service).
- Notice of Errors. In the event of any breach of the warranties in Section 6.1, the Client must tell Licensor within the relevant Warranty Period.
- Disclaimer of Warranties. Except with respect to non-infringement, and except as expressly provided in this section 6, Licensor does not make, and hereby disclaims, any and all other express or implied warranties with respect to the Licensed Software, , or otherwise related to this Agreement or its obligations hereunder, including, but not limited to, warranties of merchantability, and fitness for a particular purpose. Licensor does not warrant that the software or licensed software will be uninterrupted, error-free, or completely secure.

12. Limitation of Liability

- In no event shall either party be liable for any special, incidental, indirect, consequential or punitive damages, including but not limited to lost profits or for revenues or damages from any interruption of business, regardless of whether such party has been previously advised of the possibility of such damages.
- EXCEPT WITH RESPECT TO LICENSOR'S INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT, LICENSOR'S TOTAL AGGREGATE LIABILITY TO THE CLIENT (WHETHER IN CONTRACT, TORT, INCLUDING NEGLIGENCE, OR OTHERWISE) IN RESPECT OF EVENTS ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT SHALL BE LIMITED TO THE TOTAL AMOUNT PAYABLE BY THE CLIENT FOR LICENSED SOFTWARE IN THE MOST RECENT 12 MONTH PERIOD UNDER THE TRANSACTION DOCUMENT.

CLIENT'S TOTAL LIABILITY TO LICENSOR FOR ACTUAL DAMAGES FOR ANY CAUSE WHATSOEVER WILL BE LIMITED TO THE AMOUNT PAYABLE BY CLIENT FOR LICENSED SOFTWARE IN THE MOST RECENT 12 MONTH PERIOD UNDER THE TRANSACTION DOCUMENT.

13. Confidentiality and data protection

- The term "Confidential Information" will include information which is either marked as being confidential or which, due to the nature of the information or the circumstances under which it was disclosed, ought reasonably to be treated as confidential information of the party disclosing it. All non-public information regarding the Licensed Software and the content of the Documentation will be treated as the Confidential Information of Licensor. All data and information of the Client, including without limitation all text, sound, software, images, video files, or other materials that are required for or related to the Client's use and/or support of the Licensed Software or provided to Licensor by or on behalf of Client, will be treated as the Confidential Information of Client...
- The party receiving any of the other's Confidential Information must not:
 - use the information except to the extent necessary to enable it to perform its obligations or exercise its rights under this Agreement; or
 - disclose the information to any third party except (i) to the extent expressly allowed by this Agreement; or (ii) if required by law; but only after it notifies the other party (if legally permissible) to enable the other party to review, and, as it deems necessary, to seek a protective order or take other action.
- The provisions of this Section 8 shall survive the termination of this Agreement. Notwithstanding Section 8.1 above, the term "Confidential Information" does not include any information that:
 - is in the possession of the State and subject to disclosure under the Michigan Freedom of Information Act (FOIA);
 - is already in the public domain or enters it other than as a result of any unauthorized disclosure;
 - or
 - lawfully comes into the possession of the recipient party from a third party without the imposition of any duty of confidentiality.

14. Intellectual Property Rights

- Ownership. Licensor and its licensors own and shall retain all proprietary rights, including any and all patent, copyright, trade secret, trademark and other intellectual property rights, in and to the Licensed Software delivered to Client under this Agreement. All rights to the Licensed Software not expressly licensed to Client in this Agreement are reserved and retained by Licensor. Client acknowledges that the license granted under this Agreement does not provide it with title to or ownership of the Licensed Software, but only a right of limited use under the terms and conditions of this Agreement. Except for the rights expressly granted herein, no other rights are granted to Client with respect to the Licensed Software and all rights, title and interest in the Licensed Software shall at all times remain the property of Licensor or its licensors. , Client shall have no rights to the source code for the Licensed Software and Client agrees that, except to the extent otherwise required or permitted by law, only Licensor shall have the right to maintain, enhance, or otherwise modify the Licensed Software.
- Proprietary Markings. Licensor may affix from time to time such Licensor copyright, trademark, patent, confidentiality, and/or other notices, marks or legends on Licensed Software or a portion thereof. Client shall not knowingly remove, erase or modify any such notices, marks or legends appearing on or as part of such Licensed Software or any portion thereof.
- Documentation. Licensor will provide the Documentation in English. The Client is allowed to translate the Documentation into any other language in order to support the Client's use of the Licensed Software. Licensor is not responsible (as between the Client and Licensor) for the accuracy of any such translation. The Client must carry out any such translation itself and may not sub-license this right unless Licensor agrees otherwise (in which case it may impose reasonable conditions on such consent, for example that the sub-licensee enters an agreement direct with Licensor to protect the confidentiality of the Documentation).

15. Indemnification

- Indemnification of Client by Licensor. Licensor shall defend, indemnify and hold harmless the Client and its officers, directors, agencies, and employees (collectively, the "Indemnified Parties") from and against any and all damages, penalties, judgments and related costs and expenses, including but not limited to reasonable legal fees and expenses, ("Damages") arising out of any third party action, claim, suit, proceeding, or allegation (each a "Claim") brought against Client or any other Indemnified Party alleging that any Licensed Software or Documentation, or the use thereof by Client or any other Indemnified Party, infringes, misappropriates or violates any patent, copyright, trade secret, trade mark or any other intellectual property right of a third party, .

Unless the claim arose against the Licensed Software independently of any of the following actions, Licensor will have no liability for any claim of infringement arising solely from (i) any modifications made to the Licensed Software by Client or any third party without the knowledge or approval of Licensor; and/or (ii) Client's use of the Licensed Software in combination with other software, works or services not supplied by Licensor and not required by the Documentation and where such combination was not within the reasonable contemplation of the parties given the intended use of the Licensed Software as reflected in the Documentation or the Documentation refers to such a combination. Should the Licensed Software become, or in Licensor's opinion, be likely to become the subject of a claim or an injunction preventing their use as contemplated herein, Licensor shall either, in its discretion, (1) procure for Client the right to continue, as applicable, using such Licensed Software, (2) replace or modify the Licensed Software so that they become non-infringing (provided that such replacement or modification operates to a standard similar in all material respects to the Licensed Software concerned as to such replacement or modification), or, (3) if Licensor determines, in its sole discretion, that (1) and (2) are not commercially practical for Licensor, then Client shall return the Licensed Software for a refund of all license fees paid under the Transaction Document depreciated on a three (3) year straight line basis from the date of delivery of such Licensed Software and Licensor will refund all prepaid fees under the Transaction Document for such Licensed Software; and any licenses granted under Section 2 shall terminate .

- Reserved.
- Indemnification Procedures. If Client intends to claim indemnification under Section 10.1 (for itself or for another permitted indemnitee), then Client shall promptly notify the Licensor of such Claim, and the Licensor shall assume the defense of such Claim with counsel of the Licensor's choice. The failure of the State to deliver notice to Licensor within a reasonable time shall not relieve Licensor of its obligations hereunder except to the extent it is materially adversely prejudiced thereby. The State will provide reasonable assistance in the defense of the claim to Licensor. The State is entitled to: (a) regular updates on proceeding status; (b) participate in the defense of the proceeding; and (c) employ its own counsel. Licensor will not, without the Client's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment that requires the State to pay money, admit fault, or otherwise involves the rights of the State or its employees. Any litigation activity on behalf of the State or any of its subdivisions under this Section 10 must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.
- This Section 10 states the entire liability of Licensor with respect to infringement of third party intellectual property rights by the Licensed Software or any part thereof or by their operation.

16. Fees and payments

- License Fees and Payment. Client will make all payments to Reseller. The Client is not responsible for any delays, errors or failure of payments from its Reseller to Licensor.

17. Reserved.

18. Term and termination

- Term. This Agreement shall commence on the Effective Date and continue until terminated in accordance with this Section 13 or as otherwise specified in this Agreement (the "Term"), and the term of each individual license granted under this Agreement is perpetual, subject to the earlier termination provisions provided herein. .
- Termination. Each party may by written notice to the other terminate this Agreement or an individual license granted hereunder if:

any failure by Client to pay Reseller for Licensed Software in accordance with the Transaction Document will constitute a material breach;

the other party is in material breach (except for Client's excess use) of any of the terms of this Agreement and:

the party in breach has not rectified it within 60 days of being notified of the breach and asked to rectify it by the party not in breach; or

the other party suffers an Insolvency Event; or

by mutual agreement of the parties.

- Effect of Termination. On termination of this Agreement, or an individual license hereunder, for any reason:

Reserved.

Licensor shall be under no further obligation to supply any further services (if the overall Agreement is terminated) or the relevant Licensed Software.

the rights of the Client to use the relevant Licensed Software and Documentation shall terminate;

within 10 days of the date of termination, the Client must erase all copies of the relevant Licensed Software and, to the extent that they are not contained on media that forms an integral part of equipment belonging to the Client, return to Licensor all copies of the relevant Licensed Software and relevant Documentation and shall provide written certification to Licensor certifying that this has been done. The Client shall not be expected to return any data which Licensor does not have rights to under this Agreement or otherwise; and

Licensor will provide such reasonable support to the Client as may be required to ensure that Section 13.3(d) has been complied with.

Except for termination of this Agreement by Licensor for your material breach, all individual licenses not terminated shall survive any termination of this Agreement and such use will continue in accordance with the provisions of this Agreement.

- Survival. Sections 2.3, 6.5, 7, 8, 9.1, 9.2, 10, 13.3, 13.4, and 14, and any other terms which by their nature are intended to survive termination, shall survive any termination of this Agreement in accordance with their terms.

19. General

- U.S. Federal acquisition. This provision applies to all acquisitions of the Software and Documentation by, for, or through the U.S. Government and only to such acquisitions. By accepting delivery of the Software and/or Documentation, the U.S. Government hereby agrees that this Software and/or Documentation qualifies as commercial computer software or commercial computer software documentation as such terms are used or defined in FAR 12.212, DFARS Part 227.72, and DFARS 252.227-7014(a)(1) and (2). Accordingly, only those license rights specified in this Software License Agreement shall pertain to and govern the use, modification, reproduction, release, performance, display, and disclosure of the Software and Documentation by the U.S. Government (or other entity acquiring for or through the U.S. Government). Where any contractual terms and conditions of this Software License Agreement conflict with, or are inconsistent with, U.S. Federal Acquisition Regulation (FAR) contract clauses that apply to the U.S. Government's purchase of this Software and/or Documentation, the FAR contract clauses shall supersede any such conflicting contractual terms and conditions.
- Reserved.
- Assignment and sub-contracting. Except for an assignment required by law, neither this Agreement nor any rights under this Agreement may be assigned, sub-licensed or otherwise transferred (including by operation of law) by either party without the prior consent of the other party, such consent not to be unreasonably withheld or delayed, provided that Licensor shall be allowed to assign this Agreement to a successor to its business in connection with a merger or sale or all or substantially all of its assets.
- Notice. Any notice or other communication to be given under this Agreement shall be in writing, in English, and delivered or sent by either (a) internationally recognized courier or (b) e-mail or other electronic communication to the below addresses or (c) by mail:

If to Licensor, then:

1150 Roberts Blvd
Kennesaw,
GA 30144
e-mail: legal@nlyte.com

If to Client, then:

Shannon Romein
320 S Walnut St #6
Lansing, MI 48933
Romeins@michigan.gov
517-898-8102

Notices shall be deemed given and received in the case of notices sent by courier, when verified by written receipt; for notices sent by electronic communication when verified by automated receipt party or electronic logs ; and for notices sent by mail when actually received without verification of receipt. Where this Agreement requires or refers to something being agreed between the parties, then unless this Agreement says otherwise that agreement has to be in writing in order to be effective.

- Reserved.
- Governing Law; Venue. This Agreement (if and as varied and/or supplemented from time to time) shall be governed by and construed in accordance with the laws of Michigan, without regard to the conflicts of laws principles thereof. Other than as necessary to enforce any final judgment, award or determination, any action brought pursuant to or in connection with this Agreement shall be brought only in the state or federal courts within the State of Michigan and both parties submit to the personal jurisdiction, and waive any objections to venue, of such courts.
- Entire Agreement. This Agreement constitutes the entire agreement between the parties about the subject matter of this Agreement and supersedes all earlier understandings and agreements between either of the parties and all earlier representations by either party about such subject matter. The parties have not entered into this Agreement in reliance upon any representation, warranty or promise and no such representation or warranty or any other term is to be implied in it whether by virtue of any usage or course of dealing or otherwise except as expressly set out in it. This Agreement may not be modified except in writing signed by a duly authorized representative of both parties.
- Waiver of Compliance. Neither party shall by mere lapse of time, without giving notice or taking other action hereunder, be deemed to have waived any breach by the other party of any of the provisions of this Agreement.

Further, the waiver of either party of a particular breach of this Agreement by the other shall not be construed as or constitute a continuing waiver of such breach or of other breaches of the same or other provisions of the Agreement.

- Invalidity and Severability. In the event that all or any part of the terms, conditions or provisions contained in this Agreement are determined to be invalid, unlawful or unenforceable to any extent by any arbitrator or any court or tribunal of competent jurisdiction, such term, condition or provision shall be severed from the remaining terms, conditions and provisions which shall continue to be valid and enforceable to the fullest extent permitted by law.
- Non-Exclusive Arrangement. Licensor is free to provide services or other supplies to any other person in relation to any matter covered by this Agreement. Nothing in this Agreement shall restrict Licensor from doing so. Nothing contained in this Agreement is intended nor is to be construed as creating any requirements contract with Licensor, nor does it provide Licensor with a right of first refusal for any future work. This Agreement does not restrict the State or its agencies from acquiring similar, equal, or like services or supplies from other sources.
- Independent Parties. Nothing in this Agreement shall be construed to constitute either of the parties hereto as a partner, joint venturer, agent, representative or employee of the other party.
- Counterparts. This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which shall constitute one and the same instrument.
- Interpretation. In this Agreement, unless it says otherwise: (a) reference to a person includes a legal person (such as a limited company) as well as a natural person; (b) reference to "including" or "for example" in this Agreement shall be treated as being by way of example and shall not limit the general applicability of any preceding words; (c) reference to any legislation shall be to that legislation as amended, extended or re-enacted from time to time and to any subordinate provision made under that legislation; (d) references to a Schedule or Appendix shall mean a schedule or appendix to this Agreement; (e) section headings are inserted for ease of reference only and shall be given no effect in the construction of this Agreement; and (f) reference to this Agreement shall include reference to it after it has been amended, added to or replaced by a new Agreement. Any software supplied or licensed under this Agreement will not be treated as goods.

SCHEDULE 1

DEFINITIONS

In this Agreement the following terms shall have special meanings:

Term	Meaning
"Documentation"	The user and technical documentation for the Licensed Software delivered to Client by Licensor with the Licensed Software.
"Implementation Services"	Means the installation, configuration, training, and/or other related services that may be described in an Appendix to this document (if any) related to the implementation of the Licensed Software.
"Insolvency Event"	Means, with respect to either party, any of the following: (i) makes a general assignment for the benefit of creditors, (ii) files a voluntary petition of bankruptcy, (iii) suffers or permits the appointment of a receiver for its business or assets, (iv) becomes subject to any proceedings under any bankruptcy or insolvency law, whether domestic or foreign, which is not dismissed within sixty (60) days, or (v) has been dissolved, liquidated, or ceased doing business.
"License Fee"	The license fee payable for Licensed Software (including any license fee increments associated with increased Licensed Capacity usage).
"Licensed Capacity"	Defined in Appendix 1.
"Licensed Software"	Any software to be supplied or licensed by Licensor as described in Appendix 1. Licensed Software includes any updated, modified or replacement version of Licensed Software that may be supplied to the Client.
"Maintenance and Support Services"	The services to be supplied by Licensor under the Maintenance and Support Terms.
"Material Error"	Any defect in the Licensed Software or Documentation has a material adverse effect on its use or operation for the purpose for which it was designed or intended under this Agreement.
"New Product "	A New Product is Licensed Software that has never existed before. Any product with a new name is considered a "new product", even if some of its content existed in an old product.
"Product Release"	A numbered substantial release to a Product Version that contains material enhancements to the Licensed Software's functionality or architecture.
"Product Version"	A numbered version of the Licensed Software. A Product Version may contain multiple Product Releases.
"Reseller"	Means JEM Computers, Inc. d/b/a JEM Tech Group,
"Transaction Document"	The State's Contract No. _____ with Reseller.
"Update"	A software patch or a corrected or updated version of a Licensed Software product. The term "Update" excludes Product Versions.
"Warranty Period"	The warranty period is defined in Section 6.1 of the Agreement.

SCHEDULE 2

MAINTENANCE AND SUPPORT TERMS

General

The terms in this Schedule 2 apply to the supply of services in relation to the maintenance and support of Licensed Software. They apply in addition to the terms in the main body of the Agreement.

Maintenance and Support Services

The Maintenance and Support Services will be provided for the following periods:

the service will start on the delivery of the Licensed Software.

Releases

Licensor may produce Updates, Product Releases and Product Versions from time to time and such Updates Product Releases and Product Versions will be supplied to the Client free of charge.

New Products will be made from time to time by Licensor and the Client will be offered the opportunity to purchase New Products.

Maintenance and Support Services will only be provided in respect of:

the version of the latest Product Release (i.e. as updated with all Updates released by Licensor to the Client);
and

the one immediately before that, up to the end of a period of eighteen months from the date of first availability of the latest Product Release.

Termination

Either party may terminate the Maintenance and Support Services, without affecting this Agreement as a whole, by giving the other party 180 days written notice.

Either party may terminate the Maintenance and Support Services without terminating this Agreement as a whole if the other party is in material breach of any of the terms of this Agreement in relation to the Maintenance and Support Services concerned and:

the breach is not capable of being rectified; or

the breach is capable of being rectified, but the party in breach has not rectified it within 30 days of being notified or the breach and asked to rectify it by the party not in breach.

Where the Client chooses to terminate Maintenance and Support Services but later decides to reinstate provision of those Services from Licensor, the Client will be required to pay past Maintenance and Support Fees from the date the Maintenance and Support Services terminated. Licensor may also charge the Client a reasonable fee to cover its costs of reinstating the Maintenance and Support Services.

APPENDIX 1

Licensed Software

Licensed Software

For the purposes of this Agreement, the Licensed Software is any software supplied or licensed by Licensor as identified in or procured pursuant to the Transaction Document, and includes any updated, modified, or replacement version of Licensed Software that may be supplied to the Client.

Licensed Software is licensed on a perpetual basis, subject to the applicable Licensed Capacity.

Licensed Capacity

Client's use of the Licensed Software shall be subject to the following use limitations (in addition to those set forth in the Agreement), as applicable:

1. quantity of Managed Racks;
2. quantity of Points (restricted to facility equipment within the Client's datacenters in which the Managed Racks reside); and/or
3. quantity of Assets,
4. where such quantities are or will be identified in the Transaction Document (to include, without limitation any amendments and/or ordering documents executed thereunder).
5. The Client may not operate more than one production instance of the Software at any one point in time, provided, however, that the Client may operate test and backup instances in addition to the one production instance.

Materials

The Licensed Software is supplied with a number of Materials.

Definitions

The following defined terms apply:

“Asset”	means an entity that represents a current or planned, physical, infrastructure or IT device within an information technology environment, including properties and relationships with other entities and assets. An asset models a device throughout its lifecycle from pre-procurement to end of life.
“Datacentre Device”	means any floor standing data center facility infrastructure such as power distribution devices, power panels, and uninterruptible power supplies with an active or recycled status will be counted as a Managed Rack for every 10 assets.
“Managed Rack”	means: b) any asset with an active or recycled status within the Licensed Software created from a Material; c) any standardized frame identified as a rack or cabinet, floor standing device, tape Libraries, storage Units, mainframes, or enclosure in a Mounted IT device or Datacenter Device that has an external depth equal to or greater than approximately 39 inches (greater than exactly 1000 mm) and external width equal to or greater than approximately 23 inches (greater than exactly 600 mm) with an active or recycled status within the Licensed Software: d) any large floor standing equipment with an active or recycled status, exceeding approximately 27 cubic feet in volume (exceeding exactly 0.765 cubic meters), managed as a single asset in the Licensed Software will be counted as a Managed Rack , (for example, mainframes, mini-computers, tape silos, storage devices).; and e) any Datacentre Device.
“Materials”	These are images of materials, collected and provided by the Licensor as part of the Licensed Software. No warranty is provided by the Licensor on the correctness and suitability of those images. Materials supplied with the Licensed Software are: <ul style="list-style-type: none">• Servers, floor standing, Rack mounted and blades• Network devices that can be powered• Storage Peripherals• Chassis enclosures and modules
“Mounted IT Device”	means any asset whose location is within the mounting space of a Managed Rack'
“Points”	Are any physical data points that is being polled by the Licensed Software, such as but not limited to; temperature sensor, current sensor, fan status, power strip, etc.

This Agreement has been entered into on the date shown on the first page.

SIGNED for and on behalf of **AUTOMATED LOGIC CORPORATION DBA NLYTE SOFTWARE**

Print Name

Date

SIGNED for and on behalf of **STATE OF MICHIGAN DEPARTMENT OF TECHNOLOGY, MANAGEMENT AND BUDGET**

Print Name

Date

SCHEDULE I, Attachment 2 – TECHNOLOGY INDUSTRIES (EntryPoint) EULA

License Agreement

END USER LICENSE AGREEMENT FOR TECHNOLOGY INDUSTRIES SOFTWARE

IMPORTANT-READ CAREFULLY: THIS APPLICATION CONTAINS SOFTWARE PROPRIETARY TO TECHNOLOGY INDUSTRIES INC.

THIS END-USER LICENSE AGREEMENT ("EULA" OR "LICENSE") IS A LEGAL AGREEMENT BETWEEN the State of Michigan ("Licensed Party" or "End User" or "you" or "your") AND TECHNOLOGY INDUSTRIES INC FOR THE TECHNOLOGY INDUSTRIES EntryPoint(TM) Application ("SOFTWARE PRODUCT" OR "SOFTWARE COMPONENTS" OR "SOFTWARE" or "HARDWARE") identified in the Transaction Document. "Transaction Document" means Licensed Party's Contract No. 230000001430 with JEMTech, a Technology Industries. authorized reseller. This EULA is effective on the Effective Date in the Transaction Document.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The SOFTWARE PRODUCT is licensed, not sold.

1. Grant of License

Subject to the terms and conditions of this agreement, Technology Industries Inc. hereby grants to you a non-exclusive, non-transferable right to use the SOFTWARE PRODUCT as specified in your LICENSE GRANT from Technology Industries Inc. If you do not have LICENSE GRANT from Technology Industries Inc., do not install or use this software.

1(a) Term

The term of this EULA and the duration of the individual licenses granted hereunder is perpetual, unless earlier terminated as set forth herein. This EULA or an individual license granted hereunder may be terminated (a) by mutual written agreement of the parties; (b) without prejudice to any other rights, and except for excess use, Technology Industries Inc may terminate this EULA if you materially breach its terms and conditions and fail to cure such breach within (30) days following receipt of written notice thereof; or (c) without prejudice to any other rights, you may terminate this EULA if Technology Industries Inc materially breaches its terms and conditions and fails to cure such breach within (30) days following receipt of written notice thereof. All provisions of this EULA which by their nature are intended to survive the termination of this EULA shall survive such termination. In the event of

termination of an individual license for any reason, or termination of this EULA by Technology Industries Inc for your material breach, you must immediately cease using the SOFTWARE PRODUCT and destroy all copies of it. Except for termination of this EULA by Technology Industries Inc for your material breach, all individual licenses not terminated shall survive any termination of this EULA and such use will continue in accordance with the provisions of this EULA.

2. Restrictions

You may not modify, translate, reverse engineer, decompile, disassemble, or otherwise attempt to read, reconstruct or discover the source code from the binaries or any other hardware or software component of the of the

SOFTWARE PRODUCT. You may not modify, translate, reverse engineer, decompile, disassemble, or otherwise attempt to read, reconstruct or discover from any binary or any other software or hardware component the SOFTWARE PRODUCT'S source code, product design, processes, data structures, or database schema. You may not copy or otherwise reproduce or replicate any part of the SOFTWARE PRODUCT, except for backup and/or disaster recovery purposes.

You may not create derivative works based on the SOFTWARE PRODUCT, incorporate SOFTWARE PRODUCT in a commercial product or service or incorporate SOFTWARE PRODUCT as part of a deliverable software product. In addition, You may not, rent, lease, sublicense, convey, distribute or otherwise transfer rights to the SOFTWARE PRODUCT, remove any product identification, copyright, proprietary notices or labels from the SOFTWARE PRODUCT or use any license or trademarks in any manner other than as provided with the SOFTWARE PRODUCT. You shall not use the SOFTWARE to develop any software or other technology having the same primary function as the SOFTWARE, including but not limited to using the SOFTWARE in any development or test procedure that seeks to develop like software or other technology, or to determine if such software or other technology performs in a similar manner as the SOFTWARE. Any and all copies made by you as permitted under the terms of this LICENSE must contain all of the original SOFTWARE PRODUCT'S copyright, trademark or other proprietary notices and marks.

3. Ownership and Copyright

The SOFTWARE is protected by United States copyright laws and international treaty provisions. Technology Industries Inc. and its suppliers own and retain all right, title and interest in and to the SOFTWARE PRODUCT (including but not limited to any design, images, text, scripts, source code, documentation, incorporated into the SOFTWARE PRODUCT), including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. Your possession, installation, or use of the SOFTWARE does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this EULA.

4. U.S. GOVERNMENT RESTRICTED RIGHTS.

The SOFTWARE PRODUCT is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in this EULA and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013 (c)(1)(ii)(OCT 1988), DFARS 252.227-7015, FAR 12.211, FAR 12.212(a)(1995), FAR 52.227-19, or FAR

52.227-14, as applicable. Manufacturer is Technology Industries Inc., 814 King Street 3rd Floor Alexandria, VA 22314

5. NO WARRANTY

The SOFTWARE PRODUCT is provided under this LICENSE on an as-is basis. TECHNOLOGY INDUSTRIES INC makes no representations, extends no warranties of any kind, either express or implied, and assumes no responsibilities whatsoever with respect to the use by licensee of the SOFTWARE PRODUCT. There are no express or implied warranties of merchantability or fitness for a particular purpose or warranties that the use of the SOFTWARE PRODUCT will not infringe any patent, copyright, trademark, service mark or other rights.

6) LIMITATION OF LIABILITY

IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THIS SOFTWARE PRODUCT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THE FOREGOING PROVISIONS SHALL BE ENFORCEABLE TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. THE LICENSED PARTY'S AGGREGATE LIABILITY TO TECHNOLOGY INDUSTRIES, INC. FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS EULA, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, WILL BE LIMITED TO THE AMOUNT PAID BY THE LICENSED PARTY FOR THE SOFTWARE PRODUCT IN THE FIRST 12 MONTH PERIOD UNDER THE TRANSACTION DOCUMENT.

7) Entire Agreement

This LICENSE is the entire agreement between YOU and Technology Industries Inc relating to its subject matter. It supersedes all prior contemporaries or written communications, proposals, representations and warranties and prevails over any conflicting terms of any quote, order, acknowledgment or other communication between parties relating to its subject matter during the term

of this LICENSE. No modification of this LICENSE will be binding, unless in writing and signed by an authorized representative of Technology Industries Inc. and you.

8) Miscellaneous

This LICENSE including its enforceability and performance under any of its provisions will be governed by and construed in accordance with the laws of the State of Michigan without application of the principles of conflicts of law.

Notwithstanding anything else herein, the State will not be bound by any terms requiring indemnification by the State to Technology Industries Inc or any third parties; consent to arbitration; provisions regarding audits; provisions regarding remote access to State's systems; agreeing to be bound by the laws of another state or country; or to waive any claims or defenses, including governmental or sovereign immunity contained in any of the materials accompanying the SOFTWARE PRODUCTS, license agreements appearing with or in the SOFTWARE PRODUCTS, any terms in any third party materials or license agreements, or any other documents, policies, or terms located in links or documents referenced herein.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorized representatives.

TECHNOLOGY INDUSTRIES INC.

THE STATE OF MICHIGAN

Signature:
Name:
Title:
Date:

Signature:
Name
Title:
Date:

SCHEDULE I, Attachment 3 – RF CODE EULA

RF CODE LICENSE AGREEMENT

This RF Code License Agreement (“Agreement” or “License” or “T&C”) is between the State of Michigan (“**Customer**”) and RF Code, Inc. (“**RF Code**”) for the Technology (as defined below), and Documentation (as defined below), from RF Code identified in the Transaction Document. “**Transaction Document**” means Customer’s Contract No. 230000001430 with JEMTech, an RF Code authorized reseller (“**Reseller**”). This License is effective on September 1, 2023 (“Effective Date”).

The parties agree as follows:

1. DEFINITIONS

- 1.1. “**Affiliate**” means, with respect to Customer, any State of Michigan executive branch government agency, department, office, division, unit or entity that is supervised by or is part of Customer, or which supervises Customer or of which Customer is a part, or which is under common supervision with Customer.
- 1.2. “**Authorized Users**” means employees, contractors, and Affiliates of Customer for whom Customer has authorized to access and/or use the Technology and subject to the maximum number of users specified in the Transaction Document.
- 1.3. “**Cloud-Based Software**” means the cloud-based offering of the Software hosted by or on behalf of RF Code.
- 1.4. “**Documentation**” means user manuals, technical manuals, and any other materials provided by or on behalf of RF Code with the Technology, in printed, electronic, or other form, that describe the installation, operation, use, or technical specifications of the Technology.
- 1.5. “**Firmware**” means any firmware installed by or on behalf of RF Code on the Hardware, including any upgrades to the Firmware.
- 1.6. “**Hardware**” means any hardware made available by RF Code to Customer.
- 1.7. “**Intellectual Property Rights**” means patent rights (including patent applications and disclosures), copyrights (including rights in audiovisual works and moral rights), trade secret rights, rights of priority, and any other intellectual property rights recognized in any country or jurisdiction in the world.
- 1.8. “**Major Release**” means a release of the Software in which the first field of the version string is incremented (e.g., 4.0, 5.0, 6.0). Major Releases may include new features and enhancements that break backwards compatibility and/or represent major changes to how the product is used.
- 1.9. “**Minor Release**” means a release of the Software in which the second field of the version string is incremented (e.g., 4.1, 4.2, 4.3). Minor Releases include new features and enhancement requests that do not break backwards compatibility and do not represent major changes to how the product is used.
- 1.10. “**On-Premises Software**” means Software provided to Customer in object code form and installed by or on behalf of Customer on systems owned, licensed, or controlled by Customer.

- 1.11. **“Purchased Hardware”** means Hardware that is purchased by Customer to be owned by Customer.
- 1.12. **“Release”** means a Service Release, Minor Release, or Major Release.
- 1.13. **“Service Release”** means a release of the Software in which the third field of the version string is incremented (e.g., 4.0.1, 4.0.2, 4.0.2). Service Releases include bug fixes and minor changes only. These may also be referred to as “patches.”
- 1.14. **“Scope Limitations”** means any limitations on Customer’s use of the Technology specified by Reseller or RF Code in the Transaction Document, this Agreement or the Documentation.
- 1.15. **“Services”** means the Support Services and any installation services provided by RF Code to Customer under these T&C.
- 1.16. **“Ship Date”** means the date the Technology is made available to Customer, as communicated by RF Code or Reseller to Customer in a confirmation e-mail.
- 1.17. **“Software”** means the object code or cloud-based software made available by RF Code or Reseller to Customer. “Software” includes, and these T&C will apply to, any new Releases or copies of the Software that are made available by RF Code or Reseller to Customer.
- 1.18. **“Subscription”** means, with respect to Software, a time-limited license or right to access and use the applicable Software or, with respect to Hardware, a time-limited right to use the applicable Hardware and related Firmware.
- 1.19. **“Subscription Hardware”** means Hardware made available to Customer on a Subscription basis.
- 1.20. **“Subscription Software”** means Cloud-Based Software or On-Premises Software made available to Customer on a Subscription basis.
- 1.21. **“Support Services”** means the maintenance and support services described at www.rfcode.com/supportterms provided to Customer by or on behalf of RF Code under these T&C.
- 1.22. **“Technology”** means the Hardware, Software, and Firmware.
- 1.23. **“Term”** has the meaning specified in Section 5.
- 1.24. **“Warranty Period”** means the Standard Warranty Period applicable to the Technology purchased by Customer unless Customer has purchased extended warranty coverage for that Technology (**“Extended Warranty Coverage”**), in which case “Warranty Period” means the Extended Warranty Period. The **“Standard Warranty Periods”** for the Technology are as follows: (a) for the Purchased Hardware, Purchased Software, and Firmware, one year from the applicable Ship Date; and (b) for Subscription Software and Subscription Hardware, the applicable Term. The **“Extended Warranty Period”** means the applicable extended warranty period term purchased by Customer, if any.

2. ACCESS TO AND USE OF THE TECHNOLOGY AND DOCUMENTATION.

2.1. Subscription Software

- a) Cloud-Based. If Customer has purchased a Subscription to Cloud-Based Software, this Section 2.1(a) applies with respect to that Cloud-Based Software. Subject to and conditioned upon Customer's compliance with these T&C, and Customer's payment to Reseller for RF Code Technology in accordance with the Transaction Document, RF Code will provide Customer access to the applicable Cloud-Based Software during the applicable Term for use by and through its Authorized Users solely in connection with Customer's internal business governmental operations
- b) On-Premises. If Customer has purchased a Subscription to On-Premises Software, this Section 2.1(b) applies with respect to that On-Premises Software. Subject to and conditioned upon Customer's compliance with these T&C, and subject to Customer's payment to Reseller for RF Code Technology in accordance with the Transaction Document, RF Code grants to Customer, during the applicable Term, a non-transferable (except as permitted in Section 10.4), non-sublicensable, non-exclusive, limited license under RF Code's rights in the On-Premises Software to do the following, solely by and through its Authorized Users: (i) download and install one copy of the On-Premises Software on production servers operated by or on behalf of Customer; (ii) use the On-Premises Software solely for Customer's internal business governmental operations; and (iii) make a reasonable number of copies of the On-Premises Software solely for testing, backup, or archival purposes.

2.2. Purchased Software. If Customer has purchased a perpetual license to Software ("**Purchased Software**"), this Section 2.2 applies with respect to that Software. Subject to and conditioned upon Customer's compliance with these T&C, and subject to Customer's payment to Reseller for RF Code Technology in accordance with the Transaction Document, RF Code grants to Customer, a non-transferable (except as permitted in Section 10.4), non-sublicensable, perpetual (during the Term), non-exclusive limited license under RF Code's rights in the applicable Purchased Software to do the following, solely by and through its Authorized Users: (a) download and install one copy of the Purchased Software on production servers operated by or on behalf of Customer; (b) use the Software solely for Customer's internal business governmental operations; and (c) make a reasonable number of copies of the Purchased Software solely for testing, backup, or archival purposes.

2.3. Firmware. If Customer has purchased Purchased Hardware or a Subscription to Subscription Hardware, this Section 2.3 applies. Subject to and conditioned upon Customer's compliance with these T&C, and subject to Customer's payment to Reseller for RF Code Technology in accordance with the Transaction Document, RF Code grants to Customer a non-transferable (except as permitted in Section 10.4 or in the last sentence of this Section 2.3), non-sublicensable, non-exclusive limited license under RF Code's rights in the applicable Firmware to use the Firmware solely in connection with Customer's authorized use of the Hardware during the Term applicable to the Hardware purchased by Customer. Customer may transfer its rights in the Firmware installed on any Purchased Hardware to which it holds title to a third party solely in connection with transfer of ownership of that Purchased Hardware, and subject to the third party's agreement to the applicable terms in these T&C relating to Firmware and Purchased Hardware.

2.4 Documentation. Subject to and conditioned upon Customer's compliance with these T&C, and subject to Customer's payment to Reseller for RF Code Technology in accordance with the Transaction Document, RF Code grants to Customer a non-transferable (except as permitted in Section 10.4 or in the last sentence of this Section 2.4), non-sublicensable, non-exclusive limited license, during the Term applicable to the Technology purchased by Customer, under RF Code's rights in the applicable Documentation to, solely by and through its Authorized Users, make a reasonable number of copies of the Documentation and use that Documentation, in each case, solely in support of its authorized use of the applicable Technology in accordance with these T&C. Customer may transfer its rights in the Documentation related to any Purchased Hardware to which it holds title to a third party solely in connection with transfer of ownership of that Purchased Hardware.

2.5 Third Party Licenses. The Software, Firmware, and Documentation may include software, content, data, or other materials, including related documentation, that are owned by individuals other than RF Code. To the extent that RF Code incorporates any third party software, including without limitation open source software, into the Software, Firmware, and Documentation, RF Code shall have the responsibility to ensure that such Software, Firmware, and Documentation is properly licensed. Additionally the Software may contain embedded open source software components, which are provided as part of the Software and for which additional terms may be included at www.rfcode.com/thirdpartyterms.

2.6 Hardware Delivery. The Transaction Document governs delivery of the Hardware.

2.7 Subscription Hardware. Customer does not intend to purchase Subscription Hardware under this Agreement.

2.8 Purchased Hardware. If Customer has purchased Purchased Hardware, all right, title, and interest, and all risk of loss, damage, theft, or destruction to the Purchased Hardware passes to Customer pursuant to the terms of the Transaction Document.

2.9 License Verification To the extent that a License granted to the Customer is not unlimited, RF Code may request, either directly or through Reseller, written certification from the Customer regarding use of the Software for the sole purpose of verifying compliance with this **Section 2**. Such written certification may occur no more than once in any twenty-four (24) month period during the term of the Transaction Document. Customer will respond to any such request from RF Code within 45 calendar days of receipt. If the Customer's use is greater than contracted, Reseller may invoice the Customer for any unlicensed use (and related support) pursuant to the terms of the Transaction Document at the rates set forth in **the Transaction Document**, and the unpaid license and support fees shall be payable in accordance with the terms of the Transaction Document. Payment under this provision shall be RF Code's sole and exclusive remedy to cure these issues.

2.10 Payment. State's payment to Reseller constitutes payment to RFCode. The State is not responsible for any delays, errors or failure of payments from its Reseller to RFCode.

3. RESTRICTIONS; RESERVATION OF RIGHTS

- 3.1. Limitations. The Software, Firmware, Subscription Hardware, and Documentation are licensed, not sold, to Customer; are owned by RF Code and its licensors; and are protected by copyright and other laws of the United States and other jurisdictions. All copies of the Software, Firmware, Subscription Hardware, and Documentation: (a) are the property of RF Code; (b) are subject to the terms and conditions of these T&C; and (c) must include all trademark, copyright, patent and other Intellectual Property Rights notices contained in the original. Customer's right to use the Technology and Documentation is subject to the Scope Limitations and contingent upon Customer's compliance with the Scope Limitations.
- 3.2. Restrictions. Customer will not: (a) use the Technology or Documentation except as expressly permitted under the terms of these T&C and the Transaction Document; (b) reverse engineer, decompile, disassemble, modify, merge, or translate the Technology or Documentation, or attempt to discover either the layout of the Hardware or the source code of the Software or Firmware, or create derivative works of the Technology or Documentation; (c) except in connection with an assignment permitted under Section 10.4, transfer, assign, sublicense, sell, or otherwise convey any of Customer's rights to or license in the Software, Firmware (except as specified in Section 2.3), Documentation (except as specified in Section 2.4), or Subscription Hardware or under these T&C without the express written approval of RF Code; (d) remove, delete, alter, or obscure any trademarks or any copyright, trademark, patent, or other Intellectual Property Rights notices provided on or with the Technology or Documentation, including any copy; (f) use Documentation or the Technology after the applicable Term, even if the ability to use the applicable Technology or Documentation does not automatically become disabled; or (g) use the Technology or Documentation in, or in association with, the design, construction, maintenance, or operation of any hazardous environments or systems, including: (i) power generation systems; (ii) aircraft navigation or communication systems, air traffic control systems or any other

transport management systems; (iii) safety-critical applications, including medical or life-support systems, vehicle operation applications or any police, fire, or other safety response systems; and (iv) military or aerospace applications, weapons systems, or environments.

3.3. Responsibility for Use of Technology and Documentation. Customer is responsible for its Authorized Users' compliance with these T&C .

3.4. Reservation of Rights. RF Code grants to Customer a limited right to use the Software, Firmware, Subscription Hardware, and Documentation as described in these T&C. Customer will not have any rights to the Software, Firmware, Subscription Hardware, or Documentation except as expressly granted in these T&C. RF Code reserves to itself all rights in and to the Software, Firmware, Subscription Hardware, and Documentation not expressly granted to Customer in accordance with these T&C.

3.5. Security Features. The Technology may contain technological copy protection or other security features designed to prevent unauthorized use of the Technology, including features to protect against any use of the Technology that is prohibited or not expressly permitted under these T&C. Customer will not, and will not attempt to, remove, disable, circumvent, or otherwise create or implement any workaround to, any of those copy protection or security features.

4. SERVICES. The Transaction Document, governs any updates, releases, revisions or enhancements and support services provided by Reseller to Customer. RF Code's sole responsibility with respect to Support Services are as follows:

4.1. Support Services. Subject to Customer's payment of all applicable fees and compliance with its other obligations under these T&C, RF Code will make commercially reasonable efforts to perform Support Services for the Technology procured by Customer. Support Services are only available for Customers who have paid for and are currently using: (i) the most current Release; or (ii) the immediately preceding Release. Customer may be required to upgrade to the most current Release if the support issues raised by Customer have been corrected in the current Release. Customer's rights under Section 8 may be limited if Customer is not using the most recent Release.

4.2. Hardware and Firmware Upgrades. RF Code, in its sole discretion, may upgrade the Hardware to functionally equivalent product or upgrade the Firmware to newer versions from time to time by providing Customer reasonable notice. Customer will cooperate with RF Code to perform these upgrades.

5. TERM AND TERMINATION

5.1. Term. The duration of this Agreement is perpetual, subject to the earlier termination provisions provided herein. "**Term**" means the duration of time these T&C are in effect with respect to a particular aspect of an individual Technology license or purchase, which is determined as follows:

- a) With respect to Subscription Software and Subscription Hardware, the Term begins on the Ship Date for the applicable Subscription Software or Subscription Hardware and continues for the term defined in the Transaction Document, unless earlier terminated as provided herein; and
- b) With respect to Purchased Hardware or Software, the Term begins on the Ship Date of the applicable Technology and continues perpetually, unless earlier terminated as provided herein.

5.2. Notice of Material Breach or Default. Either party may terminate these T&C or an individual license granted hereunder, in whole or in part, (a) by mutual written agreement of the parties; or (b) for material breach (except for Customer's excess use) if the other party does not cure its material breach of these T&C within the later of: (i) 30 days of receiving the notice or (ii) the timeframe stated in the written notice of the material breach or default (which notice must include a statement of the facts relating to the material breach or default, the provisions of these T&C that are in material breach or default, the action required to cure the material breach or default, and the non-defaulting party's intention to terminate these T&C if the material breach or default is not cured within 30 days after the defaulting party's receipt of that notice or any later date as may be specified in the notice). Without limiting the foregoing, any failure by Customer to pay Reseller for RF Code Technology in accordance with the Transaction Document will constitute a material breach of these T&C. In addition to the rights provided in this Section 5.2, if Customer fails to pay Reseller for RF Code Technology in accordance with the Transaction Document, RF Code may, without limitation to any of its other rights or remedies, suspend access to the Software or Firmware, or suspend performance of any Services until such issue is resolved.

5.3. Termination for Insolvency. RF Code may terminate these T&C, effective immediately upon written notice, if Customer files, or has filed against it, a petition for voluntary or involuntary bankruptcy or pursuant to any other insolvency law, makes or seeks to make a general assignment for the benefit of its creditors or applies for, or consents to, the appointment of a trustee, receiver, or custodian for a substantial part of its property

5.4. Effect of Termination. In the event of termination of these T&C or an individual license for any reason, all rights and licenses granted by RF Code to the Customer to the applicable licensed Technology under this Agreement will terminate. Upon the termination of an individual license or any licensed Technology for any reason and/or this Agreement by RF Code for Customer's material breach, all rights and licenses (including any rights to Technology or Documentation) granted by RF Code to Customer with respect to such licensed Technology and/or under these T&C will terminate. Except for termination of this Agreement by RF Code for Customer's material breach, all individual licenses not terminated shall survive

any termination of this Agreement and this Agreement will survive with respect to such licenses.

5.5. Post-Termination Obligations.

- a) If these T&C are terminated for any reason, all provisions of these T&C which by their nature are intended to survive the termination of these T&C shall survive such termination.
- b) In the event of termination of an individual license for any reason, or If the Agreement is terminated by RF Code for Customer's material breach: (i) Customer must immediately cease use of the Subscription Software, Purchased Software, Subscription Hardware, Firmware, and Documentation, (ii) Customer will provide RF Code with a written certification signed by an authorized Customer representative certifying that all use of Subscription Software, Purchased Software, Subscription Hardware, Firmware, and Documentation has been discontinued, and (iii) Customer will, at its expense, securely package and ship the Subscription Hardware, complete with all components, hard copy Documentation, and related materials, back to RF Code. Customer assumes all risk of loss, damage, theft, or destruction of the Subscription Hardware during shipping until received by RF Code. If Customer fails to return the Subscription Hardware to RF Code in a timely manner, Customer will permit RF Code to enter Customer's premises to repossess the Subscription Hardware.

6. WARRANTIES AND DISCLAIMER

6.1. Reserved.

6.2. Technology Warranty. During the applicable Warranty Period RF Code warrants to Customer that: (a) the Hardware will be free from defects in materials and workmanship; (b) the Software will operate in all material respects in accordance with the applicable Documentation; and (c) the Firmware will operate in all material respects in accordance with the applicable Documentation.

6.3. Remedies.

To the fullest extent allowed under applicable law, Customer's sole and exclusive remedy and RF Code's entire liability for any non-conformities to the express limited warranties under Sections 6.2 will be as follows: RF Code will correct or replace the non-conforming Technology, which may include the delivery of a commercially reasonable workaround for the non-conformity; or if RF Code determines that repair or replacement of the applicable Technology is not commercially practicable, then terminate these T&C with respect to the non-conforming Technology and provide a pro-rata refund of any prepaid fees to Customer through Reseller, which fees Customer paid to RF Code or Reseller and which are attributable to the non-conforming portion of the Technology.

With respect to Hardware that is eligible for repair or replacement under this Section 6.3, Customer must follow RF Code's return process which is available on RF Code's website.

- 6.4. Limitations. The warranties in Sections 6.2 do not apply unless (a) the Technology is installed, implemented, and operated in accordance with the Documentation and any other written instructions supplied by RF Code; (b) Customer notifies RF Code in writing of any error within 10 days of the appearance thereof and includes sufficient example programs as may be necessary to demonstrate and reproduce the error; (c) Customer has not, or a third party has not, modified the Technology or combined the Technology with equipment or software other than that which is consistent with the Documentation; (iv) Customer or Reseller has promptly and properly installed any and all Releases made available by RF Code to Customer or Reseller; and (v) with respect to Hardware, the Hardware has not been damaged by accident or negligence on the part of Customer.
- 6.5. Disclaimer. EXCEPT FOR THE LIMITED WARRANTIES DESCRIBED IN SECTION 6.2, RF CODE MAKES NO OTHER EXPRESS OR IMPLIED WARRANTIES WITH RESPECT TO THE TECHNOLOGY, DOCUMENTATION, SERVICES, OR OTHERWISE AND SPECIFICALLY DISCLAIMS ALL IMPLIED AND STATUTORY WARRANTIES INCLUDING THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, SATISFACTORY QUALITY, AND FITNESS FOR A PARTICULAR PURPOSE AS WELL AS ANY WARRANTIES ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. IF THAT DISCLAIMER IS NOT PERMITTED BY LAW, THE DURATION OF ANY IMPLIED WARRANTIES IS LIMITED TO 90 DAYS FROM THE DATE OF DELIVERY. IN ADDITION, RF CODE DOES NOT WARRANT THAT THE TECHNOLOGY, DOCUMENTATION, OR SERVICES WILL SATISFY CUSTOMER'S REQUIREMENTS, ARE WITHOUT DEFECT OR ERROR, OR THAT THE OPERATION OF THE TECHNOLOGY WILL BE UNINTERRUPTED.

BECAUSE IT MAY NOT BE POSSIBLE FOR RF CODE TO KNOW THE EXACT PURPOSES FOR WHICH CUSTOMER ACQUIRED THE TECHNOLOGY OR ANY RELATED SERVICES UNDER THESE T&C, RF CODE HAS NO RESPONSIBILITY FOR ITS INSTALLATION AND USE AND THE RESULTS OF THAT USE. MODIFICATION OR ADDITIONS TO THE LIMITED WARRANTIES SET FORTH IN THESE T&C MAY BE MADE ONLY BY A WRITTEN AGREEMENT SIGNED BY AN AUTHORIZED AGENT OF EACH PARTY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF WARRANTIES, SO THAT LIMITATION OR EXCLUSION MAY NOT APPLY TO CUSTOMER.

7. LIMITATIONS OF LIABILITY

IN NO EVENT WILL RF CODE OR ITS LICENSORS BE LIABLE TO CUSTOMER FOR ANY CONSEQUENTIAL, SPECIAL, PUNITIVE, INCIDENTAL, OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF OR IN CONNECTION WITH THE TECHNOLOGY, DOCUMENTATION, OR SERVICES INCLUDING LOST PROFITS, LOSSES ASSOCIATED WITH BUSINESS INTERRUPTION, LOSS OF USE OF THE TECHNOLOGY, LOSS OF DATA, COSTS OF RE-CREATING LOST DATA, OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS, EVEN IF RF CODE HAS BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY. EXCEPT FOR (A) CLAIMS RELATED TO, BODILY INJURY, DEATH, OR PHYSICAL DAMAGE TO REAL OR TANGIBLE PROPERTY, AND (B) RFCODE'S INFRINGEMENT INDEMNIFICATION AND DEFENSE OBLIGATIONS HEREIN, IN NO EVENT WILL RF CODE'S AGGREGATE LIABILITY FOR ANY CLAIM, WHETHER IN CONTRACT, TORT OR ANY OTHER THEORY OF LIABILITY, ARISING OUT OF THESE T&C EXCEED THE TOTAL FEES PAYABLE BY CUSTOMER IN THE MOST RECENT 12 MONTH PERIOD UNDER THE TRANSACTION DOCUMENT.. Some jurisdictions do not allow the exclusion or limitation of damages, so this limitation or exclusion may not apply to Customer.

IN NO EVENT WILL CUSTOMER BE LIABLE TO RFCODE OR ITS LICENSORS FOR ANY SPECIAL, PUNITIVE, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING OUT OF OR IN CONNECTION WITH THE TECHNOLOGY, DOCUMENTATION OR SERVICES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS, EVEN IF CUSTOMER HAS BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY. IN NO EVENT WILL CUSTOMER'S AGGREGATE LIABILITY FOR ANY CLAIM, WHETHER IN CONTRACT, TORT OR ANY OTHER THEORY OF LIABILITY, ARISING OUT OF THESE T&C EXCEED THE TOTAL FEES PAYABLE BY CUSTOMER IN THE MOST RECENT 12 MONTH PERIOD UNDER THE TRANSACTION DOCUMENT.

8. INTELLECTUAL PROPERTY INDEMNIFICATION

8.1. Defense. During the Term, RF Code will defend Customer from any actual or threatened third party claim that Customer's authorized use of the Technology

infringes or misappropriates any U.S. patent issued as of the Ship Date of the Technology, or any copyright or trade secret of any third party existing as of the Ship Date of the Technology, if: (a) Customer gives RF Code prompt written notice of the claim (provided, that any failure to provide prompt notice shall not relieve RF Code of its obligations hereunder except to the extent it is materially adversely prejudiced thereby); (b) RF Code has control over the defense of the claim; and (c) Customer provides assistance in connection with the defense of the claim as RF Code may reasonably request. Notwithstanding the foregoing, the State is entitled to: (a) regular updates on proceeding status; and (b) participate in the defense of the proceeding at its own expense; (c) employ its own counsel at its own expense; and (d) retain control of the defense of Customer, at its own cost and expense, if Customer deems necessary in accordance law applicable to Customer. RF Code will not, without the State's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in that requires the State to pay money, admit fault, or otherwise involves the rights of the State or its employees(except for the right to the RF Code Technology under these T&C, which right RF Code may need to modify or terminate, in RF Code's sole discretion, due to such a third party claim) . . Any litigation activity on behalf of the State or any of its subdivisions, under this Section, must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General.

- 8.2. Indemnification. RF Code will indemnify Customer against: (a) all damages, costs, and attorneys' fees finally awarded against Customer in any proceeding under Section 8.1; (b) all out-of-pocket costs (including reasonable attorneys' fees) reasonably incurred by Customer in connection with the defense of that proceeding (other than attorneys' fees and costs incurred without RF Code's consent after RF Code has accepted defense of that claim); and (c) if any proceeding arising under Section 8.1 is settled, RF Code will pay any amounts to any third party agreed to by RF Code in settlement of those claims.
- 8.3. Mitigation of Infringement Action. If Customer's use of the Technology is, or in RF Code's reasonable opinion is likely to become, enjoined or materially diminished as a result of an actual or threatened claim or proceeding arising under Section 8.1 (which includes any settlement, including a settlement prior to a claim being filed), then RF Code will either: (a) procure the continuing right of Customer to use the Technology for the remainder of the Term; (b) replace or modify the Technology in a functionally equivalent manner so that it no longer infringes; or if, despite its commercially reasonable efforts, RF Code is unable to do either (a) or (b), RF Code will (c) terminate these T&C subject to the infringement claim and refund to Customer all unused fees pre-paid by Customer or, in the case of Purchased Software or Purchased Hardware, provide a pro rata refund based on a 5 year straight line amortization schedule.

8.4. Exclusions. RF Code will have no obligation under this Section 8 for any infringement to the extent that it arises out of or is based upon: (a) the combination, operation, or use of the Technology in conjunction with a service, hardware, or software not provided or authorized by RF Code under these T&C or the Documentation for use with the Technology if that infringement would have been avoided but for that combination, operation, or use; (b) designs, requirements, or specifications for the Technology required by or provided by Customer, if the alleged infringement would not have occurred but for those designs, requirements, or specifications; (c) use of the Technology outside of the scope provided under these T&C or the Documentation; (d) Customer's failure to use the latest Release of the Software or upgrade to the Hardware or Firmware made available to Customer by RF Code or to comply with instructions provided by RF Code, if the alleged infringement would not have occurred but for that failure; (e) any modification of the Technology not made by RF Code where that infringement would not have occurred absent that modification; or (f) unauthorized use of the Technology.

8.5. Exclusive Remedy. THIS SECTION 8 STATES RF CODE'S SOLE AND EXCLUSIVE LIABILITY, AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY, FOR THE ACTUAL OR ALLEGED INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHT BY THE TECHNOLOGY.

9. RESERVED.

10. GENERAL

10.1. Export. Customer may not export the Technology into any country prohibited by the United States Export Administration Act and the regulations thereunder. Customer acknowledges that the export of any Technology is subject to export or import control and Customer agrees that any Technology may not be exported or re-exported unless Customer obtains any required licenses to export and re-export the Technology. The Technology, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees that the Technology is not being and will not be acquired for, shipped, transferred, or re-exported, directly or indirectly, to proscribed or embargoed countries or their nationals and persons on the Table of Denial Orders, the Entity List or the List of Specifically Designated Nationals, unless specifically authorized by the U.S. Government for those purposes.

10.2. Governing Law. These T&C will be governed by the laws of the United States and the State of Michigan without regard to the conflict of laws provisions of any state or jurisdiction that would result in the application of the laws of another jurisdiction. Any litigation arising from these T&C will be brought exclusively in the state or federal courts located in Michigan. The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.

- 10.3. Reserved.
- 10.4. Assignment. Except in the event of a sale or transfer by RF Code of all or substantially all of its assets or voting securities, and except in the event of a transfer by Customer to different State of Michigan Departments, agencies, and bureaus required by law, including executive order, neither party may assign or otherwise transfer any or all of its rights, obligations or performance, these T&C or any licenses granted or obligations set forth in these T&C, without the other party's prior written consent and any attempted assignment otherwise will be null and void. These T&C are binding upon and inure to the benefit of the parties hereto and their respective permitted successors and assigns.
- 10.5. Severability. In the event that any provision of these T&C is found to be unenforceable, that provision will be enforced to the maximum extent permissible, and the validity and enforceability of the remaining provisions will not be affected thereby.
- 10.6. Waiver. Failure of either party to require performance by the other party of any provision hereof will not affect the full right to require that performance at any time thereafter; nor will the waiver by either party of a breach of any provision hereof be taken or held to be a waiver of the provision itself.
- 10.7. Entire Agreement. These T&C are the complete agreement between the parties regarding the subject matter herein. These T&C supersede and govern all previous oral and written communications regarding these matters.. These T&C may be changed only by a written agreement signed by an authorized agent of each party. Neither party will be bound by, and each party specifically objects to, any term, condition or other provision that is different from or in addition to these T&C (whether or not it would materially alter these T&C) that is contained in any purchase order, receipt, confirmation, correspondence, or other written notification or document issued by either party in relation to the Technology or Documentation hereunder.
- 10.8. U.S. Government Restricted Rights. The Software is commercial computer software, as that term is defined in 48 C.F.R. §2.101. Accordingly, if the Customer is the U.S. Government or any contractor therefor, Customer will receive only those rights with respect to the Technology and Documentation as are granted to all other end users under license, in accordance with (a) 48 C.F.R. §227.7201 through 48 C.F.R. §227.7204, with respect to the Department of Defense and their contractors, or (b) 48 C.F.R. §12.212, with respect to all other U.S. Government licensees and their contractors.
- 10.9. Relationship. The relationship between the parties is that of independent contractors. Nothing contained in this Contract is to be construed as creating any agency, partnership, joint venture or other form of joint enterprise, employment or fiduciary relationship between the parties, and neither party has authority to contract for nor bind the other party in any manner whatsoever.

- 10.10. Subcontractors. RF Code may use a subcontractor or other third party to perform its duties under these T&C and will be responsible for their performance subject to the terms of this Agreement and RF Code remains responsible for all of its obligations under these T&C.
- 10.11. Notices. Any notice required or permitted to be given in accordance with these T&C will be effective if it is in writing and sent by certified or registered mail, or insured courier, return receipt requested, or via email, to the appropriate party at the address provided by such party and with the appropriate postage affixed. Either party may change its address for receipt of notice by notice to the other party in accordance with this Section 10.11. Notices are deemed given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by email.
- 10.12. Force Majeure. Neither party will be liable for, or be considered to be in breach of or default under these T&C on account of, any delay or failure to perform as required by these T&C as a result of any cause or condition beyond such party's reasonable control, so long as such party uses all commercially reasonable efforts to avoid or remove those causes of non-performance.
- 10.13. Interpretation. Section headings are used in these T&C for convenience of reference only and will not affect the meaning of any provision of these T&C. For purposes of these T&C, (a) the words "include," "includes" and "including" will be deemed to be followed by the words "without limitation;"; (b) the words "such as", "for example" "e.g." and any derivatives of those words will mean by way of example and the items that follow these words will not be deemed an exhaustive list; and (c) the word "or" is used in the inclusive sense of "and/or" and the terms "or," "any," and "either" are not exclusive. No ambiguity will be construed against any party based on a claim that the party drafted the language. References to "purchase" of Software or Hardware refer to purchase of a limited license to use the Software or Hardware in accordance with these T&C, not purchase of the Software itself.

10.14 State Disclaimer. Notwithstanding anything else herein, Customer will not be bound by any terms requiring indemnification by the Customer to RF Code or any third parties; consent to arbitration; provisions regarding audits (which does not include the license verification clause herein); provisions regarding remote access to Customer's systems; agreeing to be bound by the laws of another state or country; or to waive any claims or defenses, including governmental or sovereign immunity contained in any of the materials accompanying the Technology or Documentation, license agreements appearing with or in the Technology or Documentation, any terms in any third party materials or license agreements, or any other documents, policies, or terms located in links or documents referenced herein.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorized representatives.

RF CODE, INC.

THE STATE OF MICHIGAN

Signature:
Name:
Title:
Date:

Signature:
Name
Title:
Date:

SCHEDULE I, Attachment 4 – MILESTONE EULA

Milestone End-user License Agreement

This End-user License Agreement (“EULA”) is a legally binding agreement between the State of Michigan Department of Technology, Management and Budget (“DTMB” or “State” or “you” or “You”) and Milestone Systems A/S (“Milestone”) setting forth the terms and conditions governing the use of the Milestone XProtect products or utilities, which may include associated software and hardware components, media, printed materials, online or electronic documentation and any updates or corrections to such documentation, identified in the Transaction Document (“Product”). “Transaction Document” means the State’s Contract No. 23000001430 with JEMTech, who has subcontracted D/A Central, Inc. a Milestone Systems A/S authorized reseller. This Agreement is effective on September 1, 2023 (“Effective Date”).

. The Product is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Note that all software parts of Product are licensed to you, not sold.

For Milestone products where a Software License Code (“SLC”) is required, the license you have been granted is identified by the Software License Code you have received when purchasing the Product.

Acceptance of Unattended Remote Updating. The system administrator of your organization may today or in the future be using a tool or operating system method enabling remote and unattended updating or installation of software products on your computer; the Milestone Software Manager is an example of such a tool. . This EULA governs the license for the use of any such Product fixes, patches, updates, new releases, revisions or enhancements if you acquire Milestone’s Care Plus and/or Care Premium for your Product licenses through the Transaction Document, other resellers, or directly from Milestone.

.No Cloud Deployment. You agree not to deploy the Product on any cloud-based infrastructure.

Intellectual Property Rights. All title and rights, including but not limited to copyrights, in and to the Product and any copies thereof are owned by Milestone, or in the case of third party contributions to such Product, the title and rights to such contributions only, are owned by our licensors. All rights not expressly granted are reserved by Milestone. The Product may include HEVC/H.265 technology that is licensed under the HEVC Advance Patent Portfolio License and the use of such technology is covered by one or more claims of the patents listed at patentlist.hevcadvance.com.

Infringement of Third Party Rights. Milestone shall be liable for ensuring that the Product does not infringe any third party's intellectual property rights, however, in respect of patents, only (a) patents granted and published in the United States of America or the European Union on the date of your purchase, and (b) only if the Product is infringing as a standalone product when not used with any other product(s) or technology unless such product(s) or technology was provided by Milestone and/or included in the Product. In the event of any action against you in which any infringement is alleged, you shall give Milestone prompt written notice thereof. Milestone shall thereafter defend at its expense and hold harmless You against any third party claim, action, or suit brought against You alleging that the Product infringes any third party’s intellectual property rights, including expenses that relate to actions for injunctive or declaratory relief.

The State will provide all reasonable assistance in the defense of the claim to Milestone. The State is entitled to:

- a. regular updates on proceeding status;
- b. participate in the defense of the proceeding;
- c. employ its own counsel; and
- d. retain control of the defense, at its own cost and expense, if the State deems necessary. Milestone will not, without the State's prior written consent (not to be unreasonably withheld), settle, compromise, or consent to the entry of any judgment in or otherwise seek to terminate any claim, action, or proceeding. Any litigation activity on behalf of the State or any of its subdivisions, under this Section, must be coordinated with the Department of Attorney General. An attorney designated to represent the State may not do so until approved by the Michigan Attorney General and appointed as a Special Assistant Attorney General

Milestone shall be entitled, at Milestone's discretion, to either obtain the continued right for you to use the Product or bring the infringement to an end by modifying or replacing the Product by another product which possesses substantially the same functionalities as the Product, or – if none of these remedies may be achieved at a reasonable cost for Milestone – to terminate this EULA with immediate effect. In the event of termination, you shall have no further claims, to include but not limited to any right of compensation or indemnity, against Milestone.

Correction of Errors. A defect or error in the Product shall be deemed material only if it has effect on the functionality of the Product as a whole or if it prevents the operation of the Product. If you, within 90 (ninety) days after purchase of the Product, document that a material defect or error in the Product exists, Milestone shall, at its sole discretion, be obligated to (i) deliver a new copy of the Product without the material defect or error, (ii) remedy or correct the defect or error free of charge, or (iii) terminate this EULA and repay any license fee received against your return of all copies of the Product. The provisions of this paragraph constitute your sole remedies in the event of a defect or error in the Product.

No Warranties. Unless you are provided with a specific warranty from Milestone as part of your Product documentation, Milestone expressly disclaims any warranty for the Product. The Product and any related documentation is provided "as is" without warranty of any kind, either expressed or implied, including, without limitation, the implied warranties of merchantability or fitness for a particular purpose. You are notified that the Product, when used with certain equipment or other software, may enable you to perform surveillance actions and data processing which are likely to be restricted by or contrary to applicable law, including without limitation data privacy and criminal law. Milestone is not responsible for verification of your use against compliance with applicable law.

Prohibited Use.

The Product may only be applied and used in accordance to the applicable law(s) of the jurisdiction, country or region it is used in. This includes, but is not limited to, possible legal restrictions to what you surveil and record with the Product, the policy for storing recorded and other data in the Product, and how such recorded data is to be handled as it is exported from the Product. Milestone is not responsible for your adherence to, such laws and restrictions. Milestone does not accept any liability whatsoever, for any direct, indirect or consequential losses or damages for the violation of such laws and/or restrictions.

Copenhagen Clause. Milestone is a signatory to the Copenhagen Letter, a technology declaration to aspire to open and honest public conversation about the power of technology and how

technology should enhance the quality of life. We who shape technology must reflect on how technology affects human needs and behaviors, and how we further the responsible use of technology. Milestone encourages our partners not only to involve themselves in this important discussion on responsible use of technology, but to also sign the Copenhagen Letter at www.copenhagenletter.org and adopt a corresponding Copenhagen Clause into their own agreements.

Limitation of Liability. The provisions of this paragraph are in effect to the maximum extent permitted by applicable law. In no event shall Milestone be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, or loss of business information) nor for any product liability (except for bodily injury) arising out of the use of or inability to use the Product or the provision of or failure to provide proper support, even if Milestone has been advised of the possibility of such damages. In no event shall the State be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss). Absent any willful misconduct or gross negligence, and except for Milestone's infringement indemnification and defense obligations herein, the entire liability of Milestone and the State shall be limited to the amount actually paid by you for the Product under the Transaction Document.

Third Party Licenses. The Products include rights for you to use certain third party software as set out in the documentation for the specific Product. You may use and integrate the Products with other third party software and Milestone is not responsible to investigate and obtain usage rights to any such third party software for your purpose.

Milestone Product Lifecycle. Your use of the Product is also subject to the Milestone Product Lifecycle, cf. <https://www.milestonesys.com/support/tools-and-references/product-lifecycle/>. In accordance with the Milestone Product Lifecycle, license activation is available for 10 years after Product's general availability. After 10 years, it may no longer be possible to add new IP devices and/or replace IP devices connected to and enabled in the Product. However, subject to this EULA, you will retain your right to use the Product and the existing XProtect system will continue to operate.

Miscellaneous. (a) You may make as many copies of the Product as may be necessary for backup and archival purposes. (b) You may not distribute copies of the Product to third parties. (c) You may not reverse engineer, decompile, or disassemble any of the Product's components except and only to the extent permitted by applicable law which cannot be contractually waived. (d) Except for an assignment required by law, this EULA is non-transferable save that if there is any ownership interest transferred which includes the Milestone Product, you may permanently assign all of your rights for this Product to the Transferee, provided the Transferee agrees to the terms of this EULA.

Termination. The term of this EULA and the duration of the individual licenses granted hereunder is perpetual, subject to the earlier termination provisions provided herein. This EULA or an individual license granted hereunder may be terminated (a) by mutual written agreement of the parties; (b) without prejudice to any other rights, and except for excess use, Milestone may terminate this EULA if you materially breach its terms and conditions and fail to cure such breach within (30) days following receipt of written notice thereof; or (c) without prejudice to any other rights, you may terminate this EULA if Milestone materially breaches its terms and conditions and fails to cure such breach within (30) days following receipt of written notice thereof. All provisions of this EULA which by their nature are intended to survive the termination of this EULA shall survive such termination.

In the event of termination of an individual license for any reason, or termination of this EULA by Milestone for your material breach, you must immediately cease using the Product and destroy all copies of it. Except for termination of this EULA by Milestone for your material breach, all individual licenses not terminated shall survive any termination of this EULA and such use will continue in accordance with the provisions of this EULA.

Severability. If a court or government body of competent jurisdiction determines that any provision of this EULA is invalid, not enforceable or enforceable only if limited in scope, this present EULA shall continue in full force and effect with such provisions stricken or so limited.

Entire Agreement. This EULA constitute the parties' entire and complete agreement relating to the subject matter hereof and all written and oral undertakings and pledges which may have preceded this EULA, all implied warranties, rules of common law or ordinary rules of law not restated herein, are hereby excluded from effect between the parties.

Governing Law. This EULA and the contract between you and Milestone are governed by Michigan law and the sole and proper forum for the settlement of disputes hereunder shall be the Michigan Court of Claims.

License, Installation and Use Conditions and Restrictions. The Product supports IP devices. IP devices can be cameras, encoders or other types of devices that are addressed through a unique IP address in the applied installation of the Product. One device license is needed per IP device connected to the Product. Each IP device connected to the Product through a network video recorder ("NVR") also requires purchase of a device license, even if such device license will not be activated in the Product, while the connecting NVR itself does not require a separate device license. IP devices with multiple lens or sensors and encoders with up to 16 connected analog cameras counts as only one IP device, due to a specific exception. Please check the list of supported IP devices at <https://www.milestonesys.com/community/business-partner-tools/supported-devices>. Specific license terms may apply for associated XProtect® branded Products, please see below for specific license terms.

Collection and registration of system data. By activating the licenses for the Product, you accept that core system data (such as number of used devices) is exchanged and stored in Milestone's licensing system which will be installed and maintained within the State's environment. A unique key for each license and each device connected to the system is generated. Milestone collects the MAC addresses of the devices connected and keeps track of the number of times cameras are registered and deleted to make sure the licenses are used according to the EULA. Milestone also registers the IP address of the server that activates the license. For systems using Milestone's push notifications, Milestone keeps track of the Globally Unique Identifier ("GUID") of the mobile server and the mobile devices that are registered to receive the notifications and email addresses that are entered to receive push notifications. The sole purpose of gathering and maintaining such data is to enable Milestone and its channel partners, to enforce license management of the Milestone products. You agree to not alter, modify, or in any way tamper with the data transmitted to the licensing service within the State's environment.

Personal Data, General Data Protection Regulation: When purchasing licenses to the Product through our channel partners, the business information of your company will be registered with

Milestone. You may need to provide Milestone with information on contact persons in form of name, email, and phone number. For the purpose of such data collection and its further use by Milestone, you may be asked to register your account in accordance with the rules specified by Milestone. If Milestone asks you to register your account, the license granted to you will not be activated before your account is registered, the required data is provided via such account and Milestone is able to authenticate you as the End-user of the Product. The purpose of gathering and maintaining such information during license usage is to enable Milestone to authenticate the End-user as a licensee of the Product, including for the purposes of export control, as well as to enable Milestone and its channel partners to enforce license management, carry out the Milestone channel programs, and provide technical support for the Product. Milestone is a data controller with respect to the personal data collected and used hereunder. Milestone treats your personal data in accordance with our Privacy Policy (<https://www.milestonestms.com/privacy-policy/>).

State Disclaimer. Notwithstanding anything else herein, the State will not be bound by any terms requiring indemnification by the State to Milestone or any third parties; consent to arbitration; provisions regarding audits; provisions regarding remote access to State's systems; agreeing to be bound by the laws of another state or country; or to waive any claims or defenses, including governmental or sovereign immunity contained in any of the materials accompanying the Products, license agreements appearing with or in the Products, any terms in any third party materials or license agreements, or any other documents, policies, or terms located in links or documents referenced herein.

This EULA applies to all Products, with its general terms and specific terms and conditions valid for the mentioned individual products as detailed in the following sections:

Milestone XProtect® VMS

Milestone XProtect® Corporate

Installation and Use – for the **XProtect Corporate** product the following applies:

Milestone hereby grants you the right to install and use the Product with the following conditions and restrictions:

1. The "Management Server" component of the Product may be installed on an unrestricted number of computers designated as Management Servers and possible clustered Management Failover Server per Software License Code.
2. The "Recording Server" component of the Product may be installed on an unrestricted number of computers designated as Recording Servers and Failover Recording Servers. The Recording Servers and Failover Recording Servers must be managed by the designated Management Server(s) specified above.
3. The Product may only be used on computers running operating systems for which the Product was designed.
4. Installing the Product you also agree to comply with Microsoft's software license terms for Microsoft SQL Server Enterprise 2019 under the State's Microsoft Enterprise Agreement .
5. The Product may, with the exceptions stated in paragraph 9 and 10 below, only be operated, regardless of whether this is directly or in some indirect form, by you, your employees or other people working for you, including law enforcement authorities investigating incidents for you. The Product may therefore, for instance, not be operated or used in any way by customers of you or other third parties.
6. The Product may only be used for surveillance of property or land that is owned or controlled by you, or you have acquired and maintain the required legal permissions when monitoring property or land not owned or controlled by you.
7. Using Milestone Federated Architecture, the Product may without being subject to additional licensing be used to connect other XProtect Corporate or XProtect Expert systems, provided that the federated system

- is rightfully licensed.
8. Using Milestone Interconnect, the Product may be used to connect other Milestone video management software products and other Milestone approved products (please refer to Milestone's web site <https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/interconnect/milestone-interconnect-compatibility/> for the latest overview of compatible products) belonging to you or a third party. The use of Milestone Interconnect is subject to the following conditions: a) any interconnected system must be fully licensed with rightfully obtained license rights, b) you through purchase or subscription have rightfully obtained Milestone Interconnect camera licenses for the cameras that shall be accessible in the XProtect Corporate system.
 9. The Product may be remotely operated and managed by a third party using Milestone Federated Architecture, provided that you have acquired and maintain the required legal permissions to conduct the surveillance.
 10. The Product may be remotely operated and managed by you or a third party using Milestone Interconnect, provided that: a) you or the third party have purchased Milestone Interconnect camera licenses for the cameras that shall be accessible in the central XProtect Corporate system, and b) you have acquired and maintain the required legal permissions to conduct the surveillance.
 11. When the Product is used with third party map applications (such as Google Maps, Microsoft® Bing™ Maps or OpenStreetMap), Milestone is not responsible to ensure that you have obtained adequate legal rights to use such map applications, and that the usage complies with the terms and conditions of the used third party applications.
 12. You acknowledge that the Product uses data from OpenStreetMap (<http://www.openstreetmap.org>) contributors. Any rights in individual contents of the database are licensed under the Database Contents License: <http://opendatacommons.org/licenses/dbcl/1.0/>. As a part of this, you also accept to respect the tile usage policy (<https://operations.osmfoundation.org/policies/tiles/>), including heavy use limitations in areas of bulk and unnecessary download of tiles.
 13. Advanced Audio Coding (AAC). Since the Product contains AAC functionality, the following provision applies: AAC is a licensed technology and as such requires a license under applicable patents in the AAC patent portfolio. The AAC license is available from VIA LICENSING CORPORATION. A limited number of AAC licenses are available through your Product from Milestone Systems. Any Milestone product that supports AAC functionality includes two viewing client licenses with the base license. When more than two viewing clients are needed, you will need to purchase additional license packs.
 14. You acknowledge the requirement that the Product may only be used with as many IP devices as you have acquired device licenses for. Please refer to the EULA general terms, "License, Installation and Use Conditions and Restrictions", stating that one device license is needed per IP camera or other IP based device connected to the system.

Milestone XProtect® Expert

Installation and Use – for the XProtect Expert product the following applies:

Milestone hereby grants you the right to install and use the Product with the following conditions and restrictions:

1. The "Management Server" component of the Product may be installed on an unrestricted number of computers designated as Management Servers and possible clustered Management Failover Server per Software License Code.
2. The "Recording Server" component of the Product may be installed on an unrestricted number of computers designated as Recording Servers and Failover Recording Servers. The Recording Servers and Failover Recording Servers must be managed by the designated Management Server(s) specified above.
3. The Product may only be used on computers running operating systems for which the Product was designed.
4. Installing the Product you also agree to comply with Microsoft's software license terms for Microsoft SQL Server 2019 Enterprise Edition under the State's Microsoft Enterprise Agreement.
5. The Product may, with the exceptions stated in paragraph 6 and 7 below, only be operated, regardless of whether this is directly or in some indirect form, by you, your employees or other people working for you, including law enforcement authorities investigating incidents for you. The Product may therefore, for instance, not be operated or used in any way by customers of you or other third parties.
6. The Product may, with the exceptions stated in paragraph 7 below, be remotely operated and managed by a third party using Milestone Federated Architecture, provided that you have acquired and maintain the required legal permissions to conduct the surveillance.
7. The Product may be remotely operated and managed by you or a third party using Milestone

- Interconnect, provided that: a) you or the third party have purchased Milestone Interconnect camera licenses for the cameras that shall be accessible in the central XProtect Corporate system, and b) you have acquired and maintain the required legal permissions to conduct the surveillance.
8. When the Product is used with third party map applications (such as Google Maps, Microsoft® Bing™ Maps or OpenStreetMap), Milestone is not responsible to ensure that you have obtained adequate legal rights to use such map applications, and that the usage complies with the terms and conditions of the used third party applications.
 9. You acknowledge that the Product uses data from OpenStreetMap (<http://www.openstreetmap.org/>)® contributors. Any rights in individual contents of the database are licensed under the Database Contents License: <http://opendatacommons.org/licenses/dbcl/1.0/>. As a part of this, you also accept to respect the tile usage policy (<https://operations.osmfoundation.org/policies/tiles>), including heavy use limitations in areas of bulk and unnecessary download of tiles.
 10. Advanced Audio Coding (AAC). Since the Product contains AAC functionality, the following provision applies: AAC is a licensed technology and as such requires a license under applicable patents in the AAC patent portfolio. The AAC license is available from VIA LICENSING CORPORATION. A limited number of AAC licenses are available through your Product from Milestone Systems. Any Milestone product that supports AAC functionality includes two viewing client licenses with the base license. When more than two viewing clients are needed, you will need to purchase additional license packs.
 11. You acknowledge the requirement that the Product may only be used with as many IP devices as you have acquired device licenses for. Please refer to the EULA general terms, "License, Installation and Use Conditions and Restrictions", stating that one device license is needed per IP camera or other IP based device connected to the system.

Milestone XProtect® Professional+

Installation and Use – for the **XProtect Professional+** product the following applies:

Milestone hereby grants you the right to install and use the Product with the following conditions and restrictions:

1. The "Management Server" component of the Product may be installed on an unrestricted number of computers designated as Management Servers and possible clustered Management Failover Server per Software License Code.
2. The "Recording Server" component of the Product may be installed on an unrestricted number of computers designated as Recording Servers. The Recording Servers must be managed by the designated Management Server(s) specified above.
3. The Product may only be used on computers running operating systems for which the Product was designed.
4. Installing the Product you also agree to comply with Microsoft's software license terms for Microsoft SQL Server 2019 Enterprise Edition under the State's Microsoft Enterprise Agreement.
5. The Product may, with the exceptions stated in paragraph 6 below, only be operated, regardless of whether this is directly or in some indirect form, by you, your employees or other people working for you, including law enforcement authorities investigating incidents for you. The Product may therefore, for instance, not be operated or used in any way by customers of you or other third parties.
6. The Product may be remotely operated and managed by you or a third party using Milestone Interconnect, provided that: a) you or the third party have purchased Milestone Interconnect camera licenses for the cameras that shall be accessible in the central Milestone XProtect Corporate system, and b) you have acquired and maintain the required legal permissions to conduct the surveillance.
7. Advanced Audio Coding (AAC). Since the Product contains AAC functionality, the following provision applies: AAC is a licensed technology and as such requires a license under applicable patents in the AAC patent portfolio. The AAC license is available from VIA LICENSING CORPORATION. A limited number of AAC licenses are available through your Product from Milestone Systems. Any Milestone product that supports AAC functionality includes two viewing client licenses with the base license. When more than two viewing clients are needed, you will need to purchase additional license packs.
8. You acknowledge the requirement that the Product may only be used with as many IP devices as you have acquired device licenses for. Please refer to the EULA general terms, "License, Installation and Use Conditions and Restrictions", stating that one device license is needed per IP camera or other IP based device connected to the system.

Milestone XProtect® Express+

Installation and Use – for the **XProtect Express+** product the following applies:

Milestone hereby grants you the right to install and use the Product with the following conditions and restrictions:

1. The "Management Server" component of the Product may be installed on one (1) computer, or cluster of computers, designated as Management Server and possible clustered Management Failover Server per Software License Code.
2. The "Recording Server" component of the Product may be installed on one (1) computer designated as Recording Server. The Recording Server must be managed by the designated Management Server specified above.
3. The Product may only be used on computers running operating systems for which the Product was designed.
4. Installing the Product you also agree to comply with Microsoft's software license terms for Microsoft SQL Server 2019 Enterprise Edition under the State's Microsoft Enterprise Agreement.
5. The Product may, with the exceptions stated in paragraph 6 below, only be operated, regardless of whether this is directly or in some indirect form, by you, your employees or other people working for you, including law enforcement authorities investigating incidents for you. The Product may therefore, for instance, not be operated or used in any way by customers of you or other third parties.
6. The Product may be remotely operated and managed by you or a third party using Milestone Interconnect, provided that: a) you or the third party have purchased Milestone Interconnect camera licenses for the cameras that shall be accessible in the central Milestone XProtect Corporate system, and b) you have acquired and maintain the required legal permissions to conduct the surveillance.
7. Advanced Audio Coding (AAC). Since the Product contains AAC functionality, the following provision applies: AAC is a licensed technology and as such requires a license under applicable patents in the AAC patent portfolio. The AAC license is available from VIA LICENSING CORPORATION. A limited number of AAC licenses are available through your Product from Milestone Systems. Any Milestone product that supports AAC functionality includes two viewing client licenses with the base license. When more than two viewing clients are needed, you will need to purchase additional license packs.
8. You acknowledge the requirement that the Product may only be used with as many IP devices as you have acquired device licenses for. Please refer to the EULA general terms, "License, Installation and Use Conditions and Restrictions", stating that one device license is needed per IP camera or other IP based device connected to the system.

Milestone XProtect® Essential+

Installation and Use – for the **XProtect Essential+** product the following applies:

Milestone hereby grants you the right to install and use the Product with the following conditions and restrictions:

1. The "Management Server" component of the Product may be installed on one (1) computer, or cluster of computers, designated as Management Server and possible clustered Management Failover Server per Software License Code.
2. The "Recording Server" component of the Product may be installed on one (1) computer designated as Recording Server. The Recording Server must be managed by the designated Management Server specified above.
3. The Product may only be used on computers running operating systems for which the Product was designed.
4. Installing the Product you also agree to comply with Microsoft's software license terms for Microsoft SQL Server 2019 Enterprise Edition under the State's Microsoft Enterprise Agreement.
5. The Product may only be used for surveillance or for other video recording purposes on property or land owned or controlled by you. The Product may therefore, for instance, not be used for surveillance of your customers' or clients' property or land.
6. In total, the Product installed under this EULA may only be used with maximum eight (8) activated IP devices. IP devices can be cameras, encoders or other types of devices that are addressed through a unique IP address in the applied installation of the Product. One device license is needed per IP device connected to the Product. Each IP device connected to the Product through an already licensed IP device also requires a device license, even if such device license will not be activated in the Product. IP devices with multiple lens or sensors and encoders with up to 16 connected analog cameras counts as only one IP device, due to a specific exception. Please check the list of supported IP devices at https://www.milestonesys.com/community/business-partner_tools/supported-devices. The Product needs to be connected to the Internet to complete the installation and to activate the license.
7. No support is provided for the Product directly from Milestone except for the support information that

can be retrieved at Milestone website as indicated to you in an information dialogue of the Product.

XProtect Clients

Milestone XProtect® Smart Client

Installation and Use – for the **XProtect Smart Client** product the following applies:

Milestone hereby grants you the right to install and use an unrestricted number of copies of the Product with the following conditions and restrictions:

1. The Product may only be used on computers running operating systems for which the Product was designed.
2. The Product may only be used in connection with a XProtect VMS product or a Milestone Husky NVR unit. When used together with a XProtect VMS product or a Milestone Husky NVR unit, the Product may also be used together with other compatible Milestone products and with third party products/components built upon the Milestone Software Development Kit or the Milestone Integration Platform Software Development Kit.
3. When used together with officially compatible Milestone products the Product may also be used together with third party products/components built upon the Milestone Integration Platform Software Development Kit
4. The use of the Product is further restricted by the End-user License Agreement of the XProtect VMS product applied.

Milestone XProtect® Web Client

Use – for the **XProtect Web Client** product the following applies:

Milestone hereby grants you the right to use the Product on an unrestricted number of computers and devices with the following conditions and restrictions:

1. Milestone XProtect Web Client includes the Milestone general terms in this EULA.
2. The Product may only be used on computers and devices running operating systems for which the Product was designed.
3. The Product may only be used together with the officially supported version of Milestone XProtect Mobile server or dedicated product evaluation environments provided by Milestone. Please see <https://www.milestonesys.com/solutions/platform/clients/xprotect-web-client/>

XProtect® Mobile

Milestone XProtect® Mobile

Installation and Use – for the **XProtect Mobile** client product the following applies:

Milestone hereby grants you the right to install and use an unrestricted number of copies of the Product with the following conditions and restrictions:

1. The Product may only be used on devices running operating systems for which the Product was designed.
2. The Product may only be used together with the officially supported version of XProtect Mobile server or dedicated product evaluation environments provided by Milestone. Please see <https://www.milestonesys.com/solutions/platform/clients/xprotect-mobile/xprotectmobilehelp/setting-up-xprotect-mobile/>
3. The use of the video push functionality is subject to licensing in the XProtect VMS product or Milestone Husky NVR unit it is used together with, where each named user of the XProtect Mobile client wanting to make use of the video push functionality requires one (1) camera license in the XProtect VMS product or Milestone Husky NVR unit.

Installation and Use – for the **XProtect Mobile** server product the following applies:

Milestone hereby grants you the right to install and use an unrestricted number of copies of the Product with the following conditions and restrictions:

1. The Product may only be used on computers running operating systems for which the Product was designed.
2. The Product may only be used in connection with a rightfully licensed XProtect VMS product or Milestone Husky NVR unit.
3. The use of the XProtect Mobile server is further restricted by the End-user License Agreement of the Milestone XProtect VMS product or Milestone Husky NVR unit it's used together with.
4. By accepting the present EULA you accept terms and conditions on behalf of end-users which you allow to connect to XProtect Mobile server in regards to use of XProtect Mobile and XProtect Web Client.
5. The use of Smart Connect, Video Push and Mobile Push notifications relies on third party services and network connectivity such as notification services and wireless communication networks. In addition to the general

restrictions in Milestone's liability defined in the section "Limitation of Liability" above, Milestone does not accept any liability arising out of the use of or inability to use any of these capabilities directly, or indirectly, caused by any of third party network or service component used to provide these capabilities.

6. The use of the Smart Connect and Mobile Push Notification capabilities is conditioned by a valid Milestone Care Plus service contract. Milestone accepts no liability for possible interruptions in the service caused by failure to renew the Milestone Care Plus coverage in due time.
7. Additional third party charges may apply for using the XProtect Mobile service, including, but not limited to, communication cost and third party service subscriptions.

Add-ons and components

Milestone XProtect® Access

Installation and Use – for the **XProtect Access** product the following applies:

Milestone hereby grants you the right to install and use the Product with the following conditions and restrictions:

1. The Product may only be used with the XProtect VMS product (any XProtect VMS product, except XProtect Essential+) or the Milestone Husky NVR unit (any Milestone Husky NVR product, except Milestone Husky M10) for which the license through purchase or subscription has rightfully been obtained.
2. The Product may be operated from an unrestricted number of XProtect Management Applications/XProtect Management Clients and XProtect Smart Clients connected to the XProtect VMS system or the Milestone Husky NVR unit.
3. To facilitate communication with third party systems an unrestricted number of XProtect Access plug-ins may be installed on the Event Server in the XProtect VMS system or the Milestone Husky NVR unit. In addition to the general restrictions in Milestone's liability defined in the section "Limitation of Liability" above, Milestone does not accept any liability arising out of the use of or inability to use the Product when the plug-ins have been provided by another party than Milestone, or when the Milestone provided XProtect Access plug-in is used with a third party product or version of a third party product that it has not been designed and validated for. Further, Milestone does not accept any liability arising out of the use of or inability to use the Product caused by errors in any third party product that XProtect Access is used together with.
4. The Product may only be used in connection with officially compatible XProtect VMS products and Milestone Husky NVR units.
5. XProtect Access may only be used with as many doors as you have purchased and registered door licenses to for the Product by the Software License Code.

Milestone XProtect® LPR

Installation and Use – for the **XProtect LPR** product the following applies:

Milestone hereby grants you the right to install and use the Product with the following conditions and restrictions:

1. The Product may only be used with the XProtect VMS product (any XProtect VMS product, except XProtect Essential+) or the Milestone Husky NVR unit (any Milestone Husky NVR product, except Milestone Husky M10) for which the license through purchase or subscription has rightfully been obtained.
2. The XProtect LPR may be installed on an unrestricted number of computers designated as XProtect LPR Servers per Software License Code.
3. The Product may only be used on computers running operating systems for which the Product was designed.
4. The Product may only be used in connection with officially compatible XProtect VMS products and Milestone Husky NVR units. When used together with officially compatible Milestone products the Product may also be used together with third party products/components built upon the Milestone Integration Platform Software Development Kit.
5. The XProtect LPR Plug-in may be installed on an unrestricted number of computers designated as Event Servers, or as Recording Servers, or on computers running the Management Client application.
6. XProtect LPR may only be used with as many cameras as you have purchased and registered LPR Camera Licenses for the Product by the Software License Code.
7. The XProtect LPR License Plate Libraries may be deployed on an unrestricted number of XProtect LPR Servers.
8. XProtect LPR may only be used with as many XProtect LPR License Plate Libraries as you have purchased and registered for the Product by the Software License Code.

Milestone XProtect® Transact

Installation and Use – for the **XProtect Transact** product the following applies:

Milestone hereby grants you the right to install and use the Product with the following conditions and restrictions:

1. The Product may only be used with the XProtect VMS product (any Milestone XProtect VMS product, except XProtect Essential+) or the Milestone Husky NVR unit (any Milestone Husky NVR product, except Husky M10) for which the license through purchase or subscription has rightfully been obtained.
2. The Product may be operated from an unrestricted number of XProtect Management Applications/XProtect Management Clients and XProtect Smart Clients connected to the XProtect VMS system or the Milestone Husky NVR unit.
3. The Product may only be used in connection with officially compatible XProtect VMS products and Milestone Husky NVR units. When used together with officially compatible Milestone products the Product may also be used together with third party products/components built upon the Milestone Integration Platform Software Development Kit.
4. The Product may only be used with as many source connections as you have purchased and registered connection licenses for under the Software License Code used by the designated XProtect Transact.

Milestone XProtect® Smart Wall

Use – for the **Milestone XProtect Smart Wall** product the following applies: Milestone hereby grants you the right to use the Product with the following conditions and restrictions:

1. The Product may be used with XProtect Corporate systems without being subject to separate licensing. The Product may be used together with XProtect Expert for which a XProtect Smart Wall base license through purchase or subscription has rightfully been obtained.
2. The Product may be operated from an unrestricted number of XProtect Management Clients and XProtect Smart Clients connected to the XProtect Corporate system.
3. The use of the Product is further restricted by the End-user License Agreement of the XProtect VMS product.

Milestone XProtect® Screen Recorder

Installation and Use – for the **Milestone XProtect Screen Recorder** product the following applies:

Milestone hereby grants you the right to install and use the Product with the following conditions and restrictions:

1. The Product may be installed on an unrestricted number of computers, and other devices, running the

- operating system for which the Product was designed (hereafter referred to as computers).
2. The Product may only be used for surveillance or for other video recording purposes of computers owned or controlled by you. The Product may therefore, for instance, not be used for surveillance of your customers' or clients' computers.
 3. The Product may only be used together with Milestone XProtect VMS products and Milestone Husky NVR units.
 4. For each use instance of the Product, one (1) camera license is required in the Milestone XProtect VMS product or Milestone Husky NVR unit.
 5. The use of the Product is further restricted by the End-user License Agreement of the Milestone XProtect VMS product or the Milestone Husky NVR unit.

Milestone XProtect® Input Unit Plug-ins

Installation and Use – for the **Milestone XProtect Input Unit Plug-ins** product the following applies:

1. The Product may only be used in connection with the Milestone XProtect Smart Client when used together with a Milestone XProtect VMS product or a Milestone Husky NVR unit, and shall be subject to the installation and use restrictions for these Products as set out in this EULA.
2. The Product may be installed on an unrestricted number of computers under one (1) Software License Code, as long as each of these computers have a valid license for the Product.

Milestone XProtect® Device Pack

Installation and Use – for the **Milestone XProtect Device Pack** product the following applies:

Milestone hereby grants you the right to install and use the Product with the following conditions and restrictions:

1. The Product and its individual Device Drivers may only be used with officially compatible and rightfully licensed Milestone XProtect VMS products or Milestone Husky NVR units.
2. The Product and its individual Device Drivers may only be used on computers running operating systems for which the Product was designed.
3. The Product and its individual Device Drivers may be installed on an unrestricted number of computers designated as Recording Servers, Failover Recording Servers or NVR units.

Milestone ONVIF Bridge

Installation and Use – for the **Milestone ONVIF Bridge** product the following applies:

Milestone hereby grants you the right to install and use the Product with the following conditions and restrictions:

1. The Product may only be used on computers running operating systems for which the Product was designed.
2. The Product may only be used in connection with a rightfully licensed Milestone XProtect VMS (except XProtect Essential+) or Milestone Husky NVR unit supporting the Milestone Integration Platform.

Milestone DirectShow Filter

Installation and Use – for the **Milestone DirectShow Filter** product (“DirectShow Filter”) the following applies: Milestone hereby grants you the right to install and use the DirectShow Filter with the following conditions and restrictions:

1. The DirectShow Filter may be installed on an unrestricted number of computers running the operating system for which the Product was designed (hereafter referred to as computers).
2. The DirectShow Filter may only be operated, regardless of whether this is directly or in some indirect form, by you, your employees or other people working for you.
3. The DirectShow Filter may only be used in connection with a Milestone XProtect VMS product, or a Milestone Husky NVR; the Product may not be used separately, in connection with non-approved Milestone products, or in connection with non-Milestone products.
4. The use of the DirectShow Filter is further restricted by the End-user License Agreement of the Milestone XProtect VMS product or the Milestone Husky NVR unit.
5. The user agrees and warrants not to knowingly use the DirectShow Filter, or other technical tools, in ways

that will enable a Milestone product to be used in a way that infringe Milestone's End-user License Agreement or licensing system for that product.

6. Even though Milestone strives to keep a high-quality level of the Product, and to make it compatible with future versions of the Products, the user of the Product understands and accepts that: a) The Product may contain incorrect, misleading or outdated material, documentation or sample products and source code. b) The Product may be incompatible with previous, present or future versions of the Milestone products. c) The Product may lack certain functionality or be incomplete in certain areas.

Milestone XProtect® Download Manager

Installation and Use – for the **Milestone XProtect Download Manager** product (“Download Manager”) the following applies:

Milestone hereby grants you the right to install and use an unrestricted number of copies of the Download Manager with the following conditions and restrictions:

1. The Download Manager may only be used on computers running operating systems for which the Download Manager was designed.
2. The Download Manager may only be used in connection with the Milestone XProtect product with which it was delivered (the Original XProtect product). When used together with the Original XProtect product the Download Manager may also be used together with other compatible Milestone products and with third party products/components built upon the Milestone Software Development Kit or Milestone Integration Platform Software Development Kit.
3. The use of the Download Manager is further restricted by the End-user License Agreement of the XProtect VMS product.

Milestone Software® Manager

Installation and Use – for the **Milestone Software Manager** utilities (“Software Manager”) the following applies: Milestone hereby grants you the right to install and use an unrestricted number of copies of the Software Manager with the following conditions and restrictions:

1. The Software Manager may only be used in connection with computers running operating systems for which the Software Manager was intended as well as in connection with computers running future operating systems Milestone may confirm to be supported by the Software Manager. Please see <https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/utilities/>
2. The Software Manager may only be used in connection with the Milestone XProtect products for which Software Manager was originally intended as well as with future products Milestone may confirm to be supported by the Software Manager. Please see <https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/utilities/>
3. By using the Milestone Software Manager to remotely install or update Milestone XProtect products on other computers you are regarded as being a system administrator of those computers (“Remote Computers”).

Husky

Milestone Husky™ X-series NVRs

Installation and Use – for the **Milestone Husky™ X-series NVRs** (covers the following products: **Milestone Husky™ X2** and **Milestone Husky™ X8**, including all variants of these products) the following applies:

Milestone hereby grants you the right to deploy and use the Product with the following conditions and restrictions:

1. The XProtect VMS software and software utilities delivered with the Product, including, but not limited to, Husky Assistant and Husky Recovery Tool, may, and can, only be used with the computer hardware and operating system with which it is delivered.
2. Product software updates and recovery images provided by Milestone for the product may, and can, only be used with the Product.

3. The Product is preloaded with XProtect VMS software. The use of the XProtect VMS software is subject to the terms and conditions for the specific product (refer to relevant section in this EULA) conditioned by the use of a rightfully obtained and registered Software License Code.
4. The Product includes an embedded Microsoft Windows Operating System. The included Microsoft Windows license gives you free access to possible updates to the Windows Operating System that Microsoft may release. Milestone is not responsible to keep the Windows Operating System current according to the Microsoft's guidelines. Milestone does not accept any responsibility for the compatibility of future software updates of the Windows Operating System, and future versions of the Microsoft Windows Operating System may change the use of available system resources in the Product, which may impact the overall performance of the Product. The Product is further dimensioned and designed for the included version of Microsoft Windows operating system. Milestone cannot guarantee the compatibility with other versions of Microsoft Windows operating systems.
5. The included Microsoft Windows Operating System must only be used together with the Product and must hence not be used on any other computer hardware. The terms and conditions for the use of the Microsoft Windows Operating System is regulated by Microsoft's end-user license agreement.

Milestone Husky™ M-series NVRs

Installation and Use – for the **Milestone Husky™ M-series NVRs** (covers the following products: **Milestone Husky™ M20, Milestone Husky™ M30 and Milestone Husky™ M50**, including all variants of these products) the following applies:

Milestone hereby grants you the right to deploy and use the Product with the following conditions and restrictions:

1. Any purchase of the Product requires prior acceptance of this EULA.
2. The Milestone Husky NVR software may, and can, only be used with the computer hardware and operating system with which it is delivered, and the Software License Code provided by Milestone. Should critical parts of the hardware need to be replaced, the software may be re-installed and activated with a new Software License Code, obtained via your Milestone dealer or from Milestone's Software Registration Service Center on Milestone's web site www.milestonesys.com.
3. The Product may, with the exceptions stated in paragraph 5 below, only be operated, regardless of whether this is directly or in some indirect form, by you, your employees or other people working for you, including law enforcement authorities investigating incidents for you. The Product may therefore, for instance, not be operated or used in any way by your customers or other third parties.
4. The Product may only be used for surveillance or for other video recording purposes on property or land owned or controlled by you. The Product may therefore, for instance, not be used for surveillance of your customers' or clients' property or land.
5. The Product may be remotely operated and managed by you or a third party using Milestone Interconnect, provided that: a) you or the third party have purchased Milestone Interconnect camera licenses for the cameras that shall be accessible in the central XProtect Corporate system, and b) you have acquired and maintain the required legal permissions to conduct the surveillance.
6. The Product has been designed for use with a maximum number of devices. Please consult your Milestone Dealer or your product documentation if you need additional information. The Product may not be used with more devices than designed for and for which you have purchased and rightfully obtained the corresponding license data for under the Software License Code.

MIP SDK and MIP SDK Mobile

Installation and Use – for the **MIP SDK** (Milestone Integration Platform Software Development Kit), and for the **MIP SDK Mobile** the following applies:

Milestone hereby grants you the right to install and use each of the Products, i.e. MIP SDK and MIP SDK Mobile, with the following restrictions:

1. The Product may be installed on an unlimited number of computers used for evaluation or

development purposes.

2. The Product may only be used on computers running operating systems for which the Product was designed.
3. The Product may only be operated, regardless of whether this is directly or in some indirect form, by you, your employees or other people working for you.
4. The Product may only be used in connection with Milestone XProtect products, Milestone Husky NVR products supporting the Milestone Integration Platform Software Development Kit, and approved OEM versions of Milestone XProtect products; the Product may not be used separately, in connection with non-Milestone products.
5. MIP SDK: You may redistribute to 3rd parties the parts of the Product which have been specifically designated as redistributable components (these are the run-time executable files contained in the following subfolders of the Product's installation folder: \bin and the \VpsSamples\bin folder), and provided that all licensing agreements, to include but not limited to those listed in the "3rd party software terms and conditions.txt" file in the \bin folder for the Product's installation folder, are included in such redistribution, in connection with your own components as a part of a total solution used together with the rightly licensed Milestone approved product.
6. MIP SDK Mobile: You may redistribute to 3rd parties the parts of the Product which have been specifically designated as redistributable components (these are the run-time executable files contained in the lib folder of every subfolder of the MIP SDK Mobile), and provided that all licensing agreements, to include but not limited to those listed in the "3rd party software terms and conditions.txt" file in the Product's installation folder, are included in such redistribution, in connection with your own components as a part of a total solution used together with the rightly licensed Milestone approved product.
7. The use of the Product is further restricted by the standard clauses mentioned in End-user License Agreement of the Milestone product, or the OEM version of the Milestone product it is used together with.
8. You agree and warrant to not knowingly using the Product, or other technical tools, in ways that will enable an end-user to use a Milestone product, or an OEM version of a Milestone product in a way that may infringe the End-user License Agreement covering the specific product, or break or circumvent the licensing system for the Milestone product or the OEM version of a Milestone product.
9. The Product includes software tools and components that enable you to connect or integrate with third party software. The Product does not include licenses for such third party software, which you must obtain yourself for your purpose.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorized representatives.

MILESTONE SYSTEMS A/S

THE STATE OF MICHIGAN

Signature:

Signature:

Name:

Name

Title:

Title:

Date:

Date:

SCHEDULE I, Attachment 5 – DIGITUS EULA

End user License Agreement (EULA)

This is a legal agreement ("Agreement") between Digitus Biometrics, Inc. and the State of Michigan ("Licensed Party" or "End User" or "you" or "your". setting forth the terms and conditions governing the use of Digitus Biometrics, Inc. proprietary software products identified in the Transaction Document (the "Software"). "Transaction Document" means Licensed Party's Contract No. 230000001430 with JEMTech, a Digitus Biometrics, Inc. authorized reseller. This Agreement is effective on the Effective Date in the Transaction Document.

1. **GRANT OF LICENSE FOR USE.** Digitus Biometrics, Inc. grants to you the non-transferable, non-exclusive, perpetual right to use and to display one copy of the software (per license issued) and any accompanying materials (the "Software") for purposes of internal or governmental, non-commercial use only. You may use the Software only on the designated number of computers, determined by the purchased license, which use may include loading the Software into a physical computer or server or a virtual computer or server. Under this license, you MAY NOT (i) distribute the Software; (ii) use the Software for any purpose other than internal or governmental, non-commercial use; or (iii) modify the Software. You may copy the Software solely for backup, disaster recovery, or archival purposes.

2. **COPYRIGHT.** The Software is owned by Digitus Biometrics, Inc. and is protected by United States copyright laws and international treaty provisions. You may not remove the copyright notice from the Software or the written materials, if any, accompanying the Software.

3. **OTHER RESTRICTIONS.** This Digitus Biometrics, Inc. License Agreement is your proof of license to exercise the rights granted herein and must be retained by you. You may not sublicense, rent or lease the Software. You may not reverse engineer, decompile or disassemble the Software except to the extent such foregoing restriction is expressly prohibited by applicable law.

4. **NO WARRANTY.** THE SOFTWARE IS PROVIDED FOR USE "AS IS" WITHOUT WARRANTY OF ANY KIND. TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGITUS BIOMETRICS, INC. AND ITS SUPPLIERS, OFFICERS, AND EMPLOYEES DISCLAIM ALL WARRANTIES OF ANY KIND, EITHER EXPRESS, STATUTORY OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. DIGITUS BIOMETRICS, INC. IS NOT OBLIGATED TO PROVIDE ANY UPDATES TO THE SOFTWARE. The Transaction Document, governs the provision of any fixes, patches, updates, new releases, revisions or enhancements and support services to the Software.

5. **DISCLAIMER AND LIMITATION OF LIABILITY FOR DAMAGES.** In no event shall either party be liable for any indirect damages whatsoever (including, without limitation, incidental, indirect, special and consequential damages, damages for loss of business profits, or business interruption, or loss of business information) arising out of the use or inability to use this Digitus Biometrics, Inc. product, even if advised of the possibility of such damages. Because some states/countries do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you. **THE LICENSED PARTY'S AGGREGATE LIABILITY TO DIGITUS BIOMETRICS, INC. FOR ANY CLAIM RELATED TO OR ARISING UNDER THIS AGREEMENT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR BY STATUTE OR OTHERWISE, WILL BE LIMITED TO THE AMOUNT PAID BY THE LICENSED PARTY FOR DIGITUS BIOMETRICS, INC. SOFTWARE IN THE FIRST 12 MONTH PERIOD UNDER THE TRANSACTION DOCUMENT.**

6. **GOVERNING LAW.** This Agreement is governed by the laws of the state of Michigan, USA without application of the principles of conflicts of law.

7. **THIRD PARTY BENEFICIARIES.** No other person or company shall be third party beneficiaries to this Agreement.

8. **PREVAILING AGREEMENT.** In the event of any conflict between the terms and conditions of this Agreement and the terms and conditions of any license agreements appearing with or in the software products comprising the Software, this Agreement shall prevail. This Agreement contains the complete agreement between the parties with respect to the subject matter herein, and supersedes all prior or contemporaneous agreements or understandings, whether oral or written and supersedes any terms. This Agreement may only be amended through a written agreement executed by a duly authorized representative of each party. If any part of this Contract is held invalid or unenforceable, by any court of competent jurisdiction, that part will be deemed deleted from this Contract and the severed part will be replaced by agreed upon language that achieves the same or similar objectives. The remaining Contract will continue in full force and effect.

9. **EXPORT.** You agree that you will not export or re-export the Software without the appropriate United States or foreign government licenses.

10. **US GOVERNMENT RESTRICTED RIGHTS.** If the Products are acquired under the terms of a proposal or agreement with the United States Government or any contractor therefore, the Products are subject to the following: (a) for acquisition by or on behalf of civilian agencies, as necessary to obtain protection as "commercial computer software" and related

documentation in accordance with the terms of this Commercial Software Agreement as specified in 48 C.F.R. 12.212 of the Federal Acquisition Regulations and its successors; (b) For acquisition by or on behalf of units of the Department of Defense ("DoD") as necessary to obtain protection as "commercial computer software" and related documentation in accordance with the terms of this commercial computer software license as specified in 48 C.F.R. 227-7202-2 of the DoD F.A.R. Supplement and its successors.

11. Disclaimer. Notwithstanding anything else herein, Licensed Party will not be bound by any terms requiring indemnification by the Licensed Party to Digitus Biometrics, Inc. or any third parties; consent to arbitration; provisions regarding audits; provisions regarding remote access to Licensed Party's systems; agreeing to be bound by the laws of another state or country; or to waive any claims or defenses, including governmental or sovereign immunity contained in any of the materials accompanying the Software, license agreements appearing with or in the software products comprising the Software, any terms in any third party materials, or any other documents, policies, or terms located in links or documents referenced herein.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorized representatives.

DIGITUS BIOMETRICS, INC

THE STATE OF MICHIGAN

Signature:
Name:
Title:
Date:

Signature:
Name
Title:
Date:

SCHEDULE I, Attachment 6 – LENEL EULA

LenelS2
1212 Pittsford-
Victor Road
Pittsford, New
York 14534
Tel 866.788.5095 Fax 585.248.9185
www.LenelS2.com



OnGuard End User License Agreement

THIS AGREEMENT (“Agreement” or “EULA”) IS A LEGAL AGREEMENT BETWEEN THE STATE OF MICHIGAN (“you” or “user” or “State”) AND CARRIER FIRE & SECURITY AMERICAS CORPORATION (“LENEL S2”). This Agreement sets forth the terms and conditions governing the use of the Software identified in the Transaction Document. Transaction Document means the State’s Contract No. Contract No. 230000001430 with JEM Computers, Inc. d/b/a JEM Tech Group (“Reseller”) _who has a subcontract relationship with D/A Central, Inc., a LENEL S2 Authorized Reseller. This Agreement is effective on September 1, 2023 (“Effective Date”)

“I”, “YOU” OR “YOUR” THROUGHOUT THE REMAINDER OF THIS EULA SHALL REFER TO THE STATE.

LENEL S2 IS WILLING TO LICENSE THE SOFTWARE AND/OR ANY SERVICE PROVIDED THROUGH THE SOFTWARE, INCLUDING ANY INTERNET OR CLOUD-BASED SERVICES (AS THE CASE MAY BE) WITH WHICH THIS EULA IS PROVIDED TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS EULA. IF YOU ACQUIRED THE SOFTWARE THROUGH ANOTHER COMPANY, PLEASE NOTE THAT LENEL S2, NOT THE OTHER COMPANY, IS LICENSING THE SOFTWARE TO YOU.

AS USED IN THIS EULA, “SOFTWARE” MEANS THE SOFTWARE PROGRAMS INCLUDED IN THE LENEL S2 ONGUARD ECOSYSTEM (INCLUDING BUT NOT LIMITED TO LNVR, ONGUARD (INCLUDING ALL VERSIONS AND ALL MODULES), ALL ONGUARD BROWSER-BASED CLIENTS (INCLUDING BUT NOT LIMITED TO THE LENEL S2 CONSOLE, ACCESS MANAGER, CREDENTIALS, MONITOR, REPORTS, SURVEILLANCE, USERS AND VISITOR CLIENTS), AND VISITOR SELF-SERVICE), AND INCLUDES ALL CORRESPONDING DOCUMENTATION, ASSOCIATED MEDIA, PRINTED MATERIALS, AND ONLINE OR ELECTRONIC DOCUMENTATION, AND ALL UPDATES OR UPGRADES OF THE ABOVE THAT ARE PROVIDED TO YOU.

Section 1. Copyright/Proprietary Protection.

The Software and all of the online help files and manuals, and all associated media, printed or electronic material included with the Software (The “Documentation”) are owned by LenelS2 and are protected by the United States and international copyright laws and other intellectual property laws and treaties. LenelS2 reserves all rights not expressly granted to you in this EULA. You must treat the Software and Documentation like any other copyrighted material, with the exceptions outlined in the following License Grant in Section 3. Any violation of this EULA may terminate your right to use the Software, subject to Section 9 below, and if such rights are terminated, you must immediately stop using the Software and return the Software to LenelS2 or uninstall and destroy all copies of the Software and Documentation in your possession (including but not limited to Software on your computers, backups and/or other devices). Upon request by LenelS2, you shall provide a written certification to LenelS2 that all such copies of the Software and Documentation have been returned and/or destroyed.

All trademarks are the property of their respective owners. You may not remove or alter any trademark, trade names, product names, logo or other proprietary notices, legends, symbols or labels in

the Software. Section 2. Third-party Software and

Additional Terms and Conditions.

The Software may contain third-party software which requires notices and/or additional terms and conditions. Such required third-party software notices and/or additional terms and conditions, if any, can be found in the OnGuard

Attributions document included in the program files\doc directory with the Software. These notices and/or additional terms and conditions are made a part of and incorporated by reference into this EULA and/or the LenelS2 product that references these notices and/or additional terms and conditions. By accepting this EULA, you are also accepting the additional terms and conditions, if any, set forth therein. Notwithstanding the foregoing or anything else herein, the State will not be bound by any terms requiring indemnification by the State to LENEL S2 or any third parties; consent to arbitration; provisions regarding audits; provisions regarding remote access to State's systems (except that remote access may only be permitted with the direct assistance and oversight of a State employee); agreeing to be bound by the laws of another state or country; or to waive any claims or defenses, including governmental or sovereign immunity contained in any of the materials accompanying the Software, license agreements appearing with or in the Software, any terms in any third party materials, or any other documents, policies, or terms located in links or documents referenced herein.

IN PARTICULAR, REGARDING H.264/AVC VISUAL STANDARD AND THE VC-1 VIDEO STANDARD, THIS PRODUCT IS LICENSED UNDER THE AVC, AND THE VC-1 PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (1) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE STANDARDS ("VIDEO STANDARDS") AND/OR (2) DECODE AVC, AND VC-1 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NO LICENSE IS GRANTED OR WILL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

Section 3. License Grant.

During the Term, as defined in Section 8 below and conditioned upon your full compliance with all of its terms, including LenelS2 grants you a , nonexclusive, nonsublicensable, revocable (only as set forth in the terminations provisions set forth in this EULA) license to install and use this Software on a single (dedicated) computer or as directed in the Documentation for your internal, governmental, non-commercial use. You may copy this Software onto the hard disk of the computer (or as directed in the Documentation), and make one copy for archival purposes. You may not make copies of the Software for any purpose other than what is stated above. LenelS2 grants you a nonexclusive, nonsublicensable, nontransferable, revocable (only as set forth in the terminations provisions set forth in this EULA) license to make and use a reasonable number of copies of the Documentation provided with the Software for your internal, governmental, non-commercial use in connection with your use of the Software; provided that you reproduce all copyright and other proprietary notices that are on the original copies. You may not reverse engineer, disassemble, decompile, decipher or attempt to discover the source code of the Software, or circumvent any technical limitations in the Software that limit or restrict access to or use of the Software or any content, file, or other work, except as expressly permitted by applicable law notwithstanding this limitation.

You may not modify the Software or create derivative works/products using this Software, in whole or in part. You may not sublicense, transfer, distribute, disclose, publish, lend, rent, lease or otherwise provide the Software or any portion of the Software to any third party, except that you may transfer your rights under this EULA on a permanent basis to another person or entity provided that you transfer this EULA, all original and updated Software and Documentation, and that you not retain any copies of the Software or Documentation. The transfer may not be an indirect transfer, such as a consignment. Before the transfer, the recipient receiving the Software must agree to all the terms and conditions of this EULA. You must promptly notify LenelS2 in writing of your transfer.

Without limiting any of the foregoing, you may not make any use of the Software in any manner not expressly permitted by this EULA. Section 4. Reservation of Rights and Ownership.

LenelS2, its affiliates, its licensors and/or its suppliers, own(s) the title, copyright and other intellectual property rights in the Software. The Software is/are protected by copyright and other intellectual property laws and treaties. Use of the Software does not transfer to you or any third party any rights, title, or interest in or to such intellectual property rights. LenelS2 and its affiliates and licensors and suppliers reserve all rights not granted in this EULA. Access to use the Software is licensed to you, not sold, under this EULA.

If the Software is not installed in a State owned, licensed, and/or controlled computer system or environment, then:

- (i) All information, files, graphics, images, documentation, communications and any other material (except Feedback, (defined below)) that you choose to submit using the Software (collectively, "User Submissions"), if any, are understood to be submitted voluntarily and will not be considered confidential or proprietary. LenelS2 does not claim ownership of User Submissions. However, by submitting, uploading, posting, or transmitting User Submissions and/or Personally Identifiable Information (as defined in Section 6 of this EULA, below) in or through the Software, you grant to

LenelS2 a worldwide, royalty-free, non-exclusive, sublicensable license to use, distribute, reproduce, modify, adapt, create derivative works of, publish, translate, publicly perform and publicly display those User Submissions in accordance with this EULA. You are solely responsible for all User Submissions uploaded, downloaded, posted, emailed, transmitted, stored or otherwise made available through the Software. LenelS2 reserves the right to determine whether any User Submission is appropriate and in compliance with this EULA, and may pre-screen, monitor, filter, restrict, block, move, refuse, modify or remove User Submissions at any time in its sole discretion, without prior notice. LenelS2 does not guarantee the security or availability of any User Submissions or other information transmitted or stored through the Software.

- (ii) You acknowledge that it is possible for LenelS2 (or any third party acting on behalf of LenelS2), in the course of providing the Software or its related services, to collect data (other than User Submissions or Personally Identifiable Information (as defined in Section 6 of this EULA, below)) that is generated by your use of the Software or its related services, or that is stored or generated by LenelS2 or the Software during your registration for or use of the Software, including but not limited to aggregated or anonymized usage data ("Usage Data"). All Usage Data shall be the property of LenelS2. LenelS2 may use Usage Data for any of its business purposes, including but not limited to the purposes of billing, providing, repairing, improving, or analyzing the Software.

You may choose to, or LenelS2 may invite you to, submit comments, suggestions, or ideas about the Software, including how to improve the Software ("Feedback"). By submitting any Feedback, you agree that any submissions are voluntary and gratuitous. Feedback is provided "as is" without any warranties including those of title and non-infringement. You irrevocably assign to LenelS2 all right, title and interest throughout the world that you may have in the Feedback without the right to any compensation or royalties from LenelS2 and, to the extent allowed by applicable law, you waive all moral rights you may have in the Feedback. LenelS2 may use, copy, modify, publish, or redistribute the Feedback, for any purpose. LenelS2 does not waive any rights to use similar or related ideas previously known to LenelS2, developed by its employees, or obtained from other sources.

LenelS2 may use or share with third parties Registration Information received in connection with registration for and use of the Software, including for its business purposes, and as required to administer, deliver, repair or improve the Software, which may include billing, collection or analytic services. Registration Information means business information about your company or government agency, including business contact information of your personnel, such as name, business telephone, address, and email, and product-related information such as product name, version, quantity, and price. LenelS2 may otherwise provide Registration Information about you, including Personally Identifiable Information (as defined in Section 6 of this EULA) that may be contained in the Registration Information that has been provided by you to LenelS2, to a third party if required by law, or in the good-faith belief that such action is necessary to comply with state and/or federal laws or respond to a court order, subpoena, or search warrant.

LenelS2 reserves the right to transfer any Registration Information LenelS2 has about you in the event LenelS2 sells or transfers all or a portion of its business or assets.

Section 5. Reserved.

Section 6. Personally Identifiable Information.

The Software may require the collection and processing of information or data that is related to any identified or identifiable natural person ("Personally Identifiable Information") to function as intended, including for the purposes of registering or managing Software, activating or deactivating Software, and providing functionality of certain internet-based services of the Software, such as BlueDiamond, as applicable. Any Personally Identifiable Information contained in your systems is owned and controlled by you. LENEL S2 has no obligation to provide notice to or obtain consent from any individuals for whom you provide Personally Identifiable Information to LenelS2, to ensure that you have the legal right to provide such information to LenelS2, and to otherwise ensure or verify your compliance with applicable data privacy laws. LenelS2, its affiliates, its licensors and/or its suppliers will retain, use, process and transfer Personally Identifiable Information in accordance with applicable data privacy laws and in accordance with the Privacy Notice available at <https://www.corporate.carrier.com/legal/privacy-notice/>.

LENEL S2 MAY MAKE CERTAIN BIOMETRIC CAPABILITIES (E.G., FINGERPRINT, VOICE PRINT, FACIAL RECOGNITION, ETC.), DATA RECORDING CAPABILITIES (E.G., VOICE RECORDING), AND/OR DATA/INFORMATION RECOGNITION AND TRANSLATION CAPABILITIES AVAILABLE IN PRODUCTS LENEL S2 MANUFACTURES AND/OR RESELLS. LENEL S2 DOES NOT CONTROL THE CONDITIONS AND METHODS OF USE OF PRODUCTS IT MANUFACTURES AND/OR RESELLS. THE END-

USER AND/OR INSTALLER AND/OR RESELLER/DISTRIBUTOR ACT AS CONTROLLER OF THE DATA RESULTING FROM USE OF THESE PRODUCTS, INCLUDING ANY RESULTING PERSONALLY IDENTIFIABLE INFORMATION OR PRIVATE DATA, AND LENELS2 IS NOT RESPONSIBLE TO ENSURE THAT ANY PARTICULAR INSTALLATION AND USE OF PRODUCTS COMPLY WITH ALL APPLICABLE PRIVACY AND OTHER LAWS, INCLUDING ANY REQUIREMENT TO OBTAIN CONSENT. THE CAPABILITY OR USE OF ANY PRODUCTS MANUFACTURED OR SOLD BY LENELS2 TO RECORD CONSENT SHALL NOT BE SUBSTITUTED FOR THE CONTROLLER'S OBLIGATION TO INDEPENDENTLY DETERMINE WHETHER CONSENT IS REQUIRED, NOR SHALL SUCH CAPABILITY OR USE SHIFT ANY OBLIGATION TO OBTAIN ANY REQUIRED CONSENT TO LENELS2.

Section 7. Additional Software or Services.

This EULA applies to any updates, supplements, add-on components, and internet-based service components (if any) of the Software that LenelS2 may, in its sole discretion, provide or make available to you ("Update"). If LenelS2 provides additional terms along with the Update, those terms will apply to the Update to the extent they do not conflict with this EULA. If LenelS2 provides you with an Update, LenelS2 may, at its sole discretion, require you to use the Update and cease use of prior versions of the Software. LenelS2 reserves the right to discontinue any internet-based service (if any) provided or made available to you through the use of the Software.

Section 8. Term of EULA.

The term of this EULA shall be perpetual ("Term") , unless earlier terminated in accordance with Section 9 or any other termination provision of this EULA.

Section 9. Termination.

LENELS2 may terminate this EULA granted hereunder upon your material breach of any of this EULA's terms and conditions and your failure to cure such breach within thirty (30) days following receipt of written notice thereof. You may terminate this EULA granted hereunder if LENELS2 materially breaches its terms and conditions and fails to cure such breach within (30) days following receipt of written notice thereof. This EULA may also be terminated by mutual written agreement of the parties.

In the event of termination of this EULA by LENELS2 for your material breach, you must immediately uninstall and destroy all copies of such Software (unless otherwise directed by LENELS2), and Sections 1, 2, 4, 6, 10, 11, 13, 14, 15 and 16 will survive.

Section 10. Limited Warranty.

LenelS2 warrants that the physical media on which the Software is distributed, if applicable, is free from defects in materials and workmanship and that the Software will function in substantial accordance to the Documentation that accompanies the Software for a period of one (1) year from the date of shipment of the Software to the reseller. This limited warranty is void if failure of the Software results from accident, abuse, modification, misapplication, misuse, abnormal use or a virus. THE WARRANTIES DESCRIBED HEREIN AND/OR ACCOMPANYING THE SOFTWARE ARE IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS AND, EXCEPT AS OTHERWISE PROVIDED HEREIN, LENELS2 AND ITS PARENT, AFFILIATES AND SUPPLIERS MAKE AND THERE ARE NO OTHER WARRANTIES OR CONDITIONS OR REPRESENTATIONS OF ANY KIND WHETHER EXPRESS OR IMPLIED, AND LENELS2, ITS PARENT, AFFILIATES AND SUPPLIERS EXPRESSLY DISCLAIM THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND THOSE ARISING BY STATUTE OR OTHERWISE IN LAW OR FROM A COURSE OF DEALING OR USAGE OF TRADE. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT, LACK OF VIRUSES OR BUGS, ACCURACY OR COMPLETENESS OF RESPONSES OR RESULTS WITH REGARD TO THE SOFTWARE. LENELS2 AND ITS PARENT, AFFILIATES AND SUPPLIERS DO NOT REPRESENT OR WARRANT THAT THE SOFTWARE WILL MEET ANY OR ALL OF YOUR PARTICULAR REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR FREE OR UNINTERRUPTED OR THAT THE SOFTWARE WILL PREVENT OR MINIMIZE OCCURRENCES OF PROPERTY DAMAGE, THEFT, LOSS OR PERSONAL INJURY. LENELS2 AND ITS PARENT, AFFILIATES AND SUPPLIERS FURTHER DISCLAIM ANY OTHER IMPLIED WARRANTY UNDER THE UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT OR SIMILAR LAW AS ENACTED BY ANY STATE.

LENELS2 DOES NOT REPRESENT THAT THE SOFTWARE OR ITS RELATED SERVICES MAY NOT BE HACKED, COMPROMISED AND/OR CIRCUMVENTED. LENELS2 DOES NOT WARRANT THAT ITS SOFTWARE OR ITS RELATED SERVICES WILL WORK PROPERLY IN ALL ENVIRONMENTS AND APPLICATIONS AND DOES NOT WARRANT ANY SOFTWARE OR ITS RELATED SERVICES AGAINST HARMFUL ELECTROMAGNETIC INTERFERENCE INDUCTION OR RADIATION (EMI, RFI, ETC.) EMITTED

FROM EXTERNAL SOURCES. THE ABILITY OF THE SOFTWARE AND ITS RELATED SERVICES TO WORK PROPERLY DEPENDS ON A NUMBER OF PRODUCTS AND SERVICES MADE AVAILABLE BY THIRD PARTIES OVER WHICH LENEIS2 HAS NO CONTROL INCLUDING, BUT NOT LIMITED TO, INTERNET, CELLULAR AND LANDLINE CONNECTIVITY; MOBILE DEVICE AND RELATED OPERATING SYSTEM COMPATIBILITY; OR PROPER INSTALLATION AND MAINTENANCE OF AUTHORIZED HARDWARE AND OTHER SOFTWARE.

FOR MORE INFORMATION ON PRODUCT WARNINGS AND DISCLAIMERS, PLEASE VISIT:

[HTTPS://FIRESECURITYPRODUCTS.COM/EN/POLICY/PRODUCT-WARNING](https://firesecurityproducts.com/en/policy/product-warning). THIS INFORMATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

LENEIS2 SHALL PROVIDE A MINIMUM SUPPORT PERIOD OF THREE (3) YEARS FOR ITS LATEST VERSION/RELEASE OF ONGUARD. USING A VERSION OF ONGUARD THAT IS NO LONGER SUPPORTED OR THAT HAS NOT BEEN UPDATED WITH AVAILABLE UPDATES CAN RESULT IN LOSS OF FUNCTIONALITY AND RESULT IN INCREASED VULNERABILITY TO UNAUTHORIZED ACCESS. SOFTWARE UPDATES AND/OR THE LATEST VERSION/RELEASE OF ONGUARD SHALL BE MADE AVAILABLE THROUGH LENEIS2 AUTHORIZED VALUE ADDED RESELLERS. THE AVAILABILITY OF SOFTWARE UPDATES AND/OR THE LATEST VERSION/RELEASE OF ONGUARD MAY NOT BE COMMUNICATED DIRECTLY BY LENEIS2 TO THE END USER.

Any written or oral information or advice given by LeneIS2 resellers, channel partners, distributors, agents or employees will in no way increase the scope of this warranty. You may have other legal rights, which vary from state to state.

Section 11. No Liability for Consequential or Incidental Damages and Limitation of Liability.

IN NO EVENT SHALL EITHER PARTY, ITS PARENTS, AFFILIATES, SUPPLIERS OR RESELLERS/CHANNEL PARTNERS BE LIABLE FOR ANY SPECIAL, PUNITIVE, INDIRECT, CONSEQUENTIAL OR INCIDENTAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, DAMAGES TO ANY COMPUTER, DEVICE OR SYSTEM, BUSINESS INTERRUPTION, LOSS OF INFORMATION/DATA, GOODWILL, USE, OTHER PECUNIARY LOSS OR ATTORNEY FEES) ARISING OUT OF OR IN ANY WAY RELATED TO THE SOFTWARE OR THIS EULA, REGARDLESS OF THE CAUSE OF ACTION OR THE BASIS OF THE CLAIM AND EVEN IF LENEIS2 OR ITS PARENT, AFFILIATES, SUPPLIERS OR RESELLERS/CHANNEL PARTNERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR REMEDIES FAIL OF THEIR ESSENTIAL PURPOSE. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. FURTHER, TO THE EXTENT PERMITTED BY LAW, IN NO EVENT SHALL EITHER PARTY'S, AFFILIATES', SUPPLIERS', RESELLERS' OR CHANNEL PARTNERS' ENTIRE LIABILITY AS TO ANY AND ALL DAMAGES ARISING OUT OF THIS EULA OR THE USE OF THE SOFTWARE EXCEED THE AMOUNT PAID BY YOU FOR THE RIGHT TO USE THE SOFTWARE. NO ACTION, REGARDLESS OF FORM, RELATING TO THE SOFTWARE MAY BE BROUGHT BY YOU MORE THAN ONE YEAR AFTER YOU HAVE KNOWLEDGE OF THE OCCURRENCE WHICH GIVES RISE TO THE CAUSE OF ACTION.

Section 12. Force Majeure.

LeneIS2 will not be in breach of this EULA or be liable if it fails to perform or delays the performance of an obligation as a result of an event beyond its reasonable control, including but not limited to, computer or mobile device operating system errors or outages, network or cellular outages, strikes, lockouts, industrial disputes, fire, flood, act of God, war, insurrection, vandalism, sabotage, invasion, riot, national emergency, epidemic, pandemic, piracy, hijack, acts of terrorism, embargoes or restraints, epidemic, legislation, regulation, order or other act of any government or governmental agency.

Section 13. U.S. Government Restricted Rights.

The Software is provided with restricted rights. Use, duplication or disclosure by the government is subject to restrictions set forth in subparagraph (b)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252-227-7013 or subparagraphs (b)(1) and (2) of the Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, as applicable.

Contractor/manufacture is Carrier Fire & Security Americas

Corporation. Section 14. Export Controls.

You acknowledge that the Software is of U.S. origin and subject to the export control laws of the United States and applicable export and import control laws of other countries. You agree to comply with and use the Software in a manner consistent with such applicable international and national laws, rules and regulations that apply to the Software and your use of the Software, including the U.S. Export Administration Regulations, as well as end user, end use, and destination restrictions issued by U.S. or other governments. All rights to use the Software are granted on the condition that such rights are forfeited if you fail to comply with this EULA.

Section 15. Governing Law and Jurisdiction.

This EULA is governed by the laws of the State of Michigan, excepting its laws concerning the selection of jurisdiction or conflict of laws, and any disputes or claims arising hereunder shall be under the exclusive jurisdiction of the state and federal courts situated in the State of Michigan. The United Nations Convention on Contracts for the International Sale of Goods does not apply to this EULA.

Section 16. General Provisions.

The section titles in this EULA are used solely for the parties' convenience and have no legal or contractual significance. Any list of examples following "including" or "e.g.," is illustrative and not exhaustive, unless qualified by terms like "only" or "solely." Either party's failure to act with respect to a breach by the other party does not waive its right to act with respect to subsequent or similar breaches. No waiver of any provision of this EULA will be effective unless it is in a signed writing, and no waiver will constitute a waiver of any other provision(s) or of the same provision on another occasion. If a court of competent jurisdiction holds any term, covenant or restriction of this EULA to be illegal, invalid or unenforceable, in whole or in part, the remaining terms, covenants and restrictions will remain in full force and effect and will in no way be affected, impaired or invalidated. This EULA will be binding upon all successors and assigns. This EULA constitutes the entire agreement between you and LenelS2 with respect to the Software and merges all prior and contemporaneous communications and proposals, whether electronic, oral or written, between you and LenelS2 with respect to the Software. This Agreement may only be amended through a written agreement executed by a duly authorized representative of each party. No LenelS2 value added reseller, dealer, distributor, agent or employee thereof is authorized to make any amendment to this EULA. All notices to either party in connection with this EULA must be in writing and will be deemed given and received: (a) when verified by written receipt if sent by courier; (b) when actually received if sent by mail without verification of receipt; or (c) when verified by automated receipt or electronic logs if sent by facsimile or email. If you have any questions about this EULA, or want to contact LenelS2 for any reason, please direct all correspondence to:

LenelS2
1212 Pittsford
Victor Road Pittsford, New York 14534 USA
Attn: Legal Department

Notices to the State will be sent to:
Shannon Romein
320 S Walnut St #6
Lansing, MI 48933
Romeins@michigan.gov
517-898-8102

Copyright and Related Notices

LENEL S2 offers Non-English versions of LenelS2 documents as a service to its global audiences. LENEL S2 has attempted to provide an accurate translation of the text, but the official text is the English text, and any differences in the translation are not binding and have no legal effect.

Product names mentioned in this document, if any, may be trademarks or registered trademarks of their respective owners and are hereby acknowledged.

Product Disclaimers and Warnings

THESE PRODUCTS ARE INTENDED FOR SALE TO, AND INSTALLATION BY, AN EXPERIENCED SECURITY PROFESSIONAL. LENEL S2 CANNOT PROVIDE ANY ASSURANCE THAT ANY PERSON OR ENTITY BUYING ITS PRODUCTS, INCLUDING ANY "AUTHORIZED DEALER", IS PROPERLY TRAINED OR EXPERIENCED TO CORRECTLY INSTALL SECURITY RELATED PRODUCTS.

IN WITNESS WHEREOF, the Parties have caused this Agreement to be executed by their duly authorized representatives.

LENEL S2

THE STATE OF MICHIGAN

Signature:

Signature:

Name:

Name

Title:

Title:

Date:

Date: